


Declaration

1. My name is Jeff Lilleskare. I am a group manager for security and online safety at Microsoft Corporation. As part of my responsibilities, I am familiar with Microsoft's processes for reporting images detected using its PhotoDNA technology to the National Center for Missing and Exploited Children (NCMEC).
2. I have reviewed the CyberTipline Reports (the "Reports") attached at **Exhibit A**. These Reports share the following common features:
 - These Reports are each submitted by Microsoft in relation to its Skype service.
 - These Reports each refer to an "original binary hash of the file (PhotoDNA)," which signifies that PhotoDNA detected the image at issue.
 - These Reports each state that the file was reviewed and categorized by the provider. This signifies that someone at Microsoft reviewed the image at issue before it was transmitted to NCMEC.
3. I also attach true and accurate copies of the following Microsoft Services Agreements and related materials at **Exhibit B**:
 - Microsoft Services Agreement Effective July 31, 2014
 - Microsoft Services Agreement Effective August 1, 2015
 - Microsoft Services Agreement Effective September 15, 2016
 - Microsoft Privacy Statement, updated June 2017
 - Microsoft Privacy Statement, Change History (as of June 2017)
4. Before a customer may create a Skype account, he or she must agree to the applicable terms of service, including the applicable Microsoft Services Agreement.



* * *

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct. Executed on 6/21/17.



Jeff Lilleskare

EXHIBIT A



CyberTipline Report 11614028

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 05-20-2016 17:09:22 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*

Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Section C: Additional Information Provided by NCMEC	4
NCMEC Note #1	4
NCMEC Note #2	4
Section D: Law Enforcement Contact Information	12
Vermont Office of Attorney General	12



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 01-01-0001 00:00:00 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
Peer to Peer Filenames: tmp8150.jpg

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename:	tmp8150.jpg
Was File Reviewed by Company?	Yes
Child Pornography Categorization by ESP: (See Section B for further explanation)	A1
Original Binary Hash of File (PhotoDNA):	10,51,0,92,35,31,3,85,23,91,10,171,71,15,5,119,13,42,0,49,17,20,8,34,36,249,13,159,93,37,0,249,48,64,20,163,113,16,24,98,33,76,1,140,72,12,4,109,5,255,96,11,26,40,28,46,29,8,8,86,146,34,13,140,60,157,44,113,179,14,18,54,1,198,146,15,3,181,88,23,8,25,31,38,80,7,24,75,101,90,58,74,134,20,59,23,0,225,7,66,4,190,17,62,19,42,44,17,60,30,43,27,172,2,65,18,60,8,150,3,0,255,18,62,10,80,39,43,39,26,62,45,38,41,64,25,209,1,41,8,94,5,53,3
Original URL Where File was Located:	D:\local\Temp\tmp8150.jpg

**Additional Information:****Where to serve legal process in Criminal Matters**

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other Online Services:

FAX: (425) 708-0096 Microsoft Corporation
Attn: Online Services Custodian of Records
One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 15:47:00 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-RHS 06-27-2016 19:40:55 UTC

Microsoft provided the following reported user information:

Screen Name: vt151231,78837c86b9c60032

IP Address: 24.91.154.58

NCMEC Note #2

ECD-NB 06-28-2016 16:02:53 UTC

I reviewed the uploaded file and found what appears to be apparent child pornography

=====

CT/TA search results for:

vt151231

78837c86b9c60032

24.91.154.58

11614028

11751258

11751259

12045016

12050728

12050735

12050739



12051516
12051925
12415510
12415511
12415578
12415755
12468560
12468566
12469951
12469960
12469962
12469964
12526149
12526150
12526151
12526152
12526153
12526155
12526156
12526157
12526159
12527752
12527760
12627552
12627584
12627589
12651690
12651697
12651701
12765571
12765579
12766078

=====

CT/TA Search results for : *jvt15123456* (from 12469951)

12468560
12468566
12469960
12469962
12469964

=====

CT/TA Search results for : *jvt1234515* (from 12527752)

12526149
12526150
12526151
12526152
12526153
12526155
12526156
12526157



12526159
12527752
12527760

=====

CT/TA Search results for : *jvt12345615* (from 12627589)

12627552
12627584
12627589
12651690
12651697
12651701

=====

CT/TA Search results for : *vtj12315* (from 12765571)

12765579
12766078

=====

CT/TA Search results for : *vt151233* (from 12050728)

12045016
12050735
12050739
12051516
12051925

=====

A WHOIS search for '24.91.154.58' yielded the following:

Address lookup

canonical name

c-24-91-154-58 . hsd1 . vt . comcast.net .

aliases

addresses

24.91.154.58

Network Whois record

Queried whois.arin.net with "n ! NET-24-91-128-0-1 "...

NetRange: 24.91.128.0 - 24.91.255.255

CIDR: 24.91.128.0/17

NetName: NEW-ENGLAND-7

NetHandle: NET-24-91-128-0-1

Parent: RW2-NORTHEAST-2 (NET-24-91-0-0-1)

NetType: Reassigned

OriginAS:

Customer: Comcast Cable Communications Holdings, Inc (C02610697)



RegDate: 2010-10-18
 Updated: 2010-10-18
 Ref: <https://whois.arin.net/rest/net/NET-24-91-128-0-1>
 CustName: Comcast Cable Communications Holdings, Inc
 Address: 1800 Bishops Gate Blvd
 City: Mt Laurel
 StateProv: NJ
 PostalCode: 08054
 Country: US
 RegDate: 2010-10-18
 Updated: 2011-03-19
 Ref: <https://whois.arin.net/rest/customer/C02610697>
 OrgAbuseHandle: NAPO-ARIN
 OrgAbuseName: Network Abuse and Policy Observance
 OrgAbusePhone: +1-888-565-4329
 OrgAbuseEmail: abuse@comcast.net
 OrgAbuseRef: <https://whois.arin.net/rest/poc/NAPO-ARIN>
 OrgTechHandle: IC161-ARIN
 OrgTechName: Comcast Cable Communications Inc
 OrgTechPhone: +1-856-317-7200
 OrgTechEmail: CNIPEO-lp-registration@comcast.com
 OrgTechRef: <https://whois.arin.net/rest/poc/IC161-ARIN>

DNS records

```

name class type data time to live
c-24-91-154-58.hsd1.vt.comcast.net IN A 24.91.154.58 7200s (02:00:00)
hsd1.vt.comcast.net IN NS dns101.comcast.net 7200s (02:00:00)
hsd1.vt.comcast.net IN NS dns104.comcast.net 7200s (02:00:00)
hsd1.vt.comcast.net IN NS dns105.comcast.net 7200s (02:00:00)
hsd1.vt.comcast.net IN NS dns103.comcast.net 7200s (02:00:00)
hsd1.vt.comcast.net IN NS dns102.comcast.net 7200s (02:00:00)
hsd1.vt.comcast.net IN SOA server: dns101.comcast.net email: dnsadmin@comcast.net serial: 1351826 refresh: 7200
retry: 3600 expire: 604800 minimum ttl: 7200 7200s (02:00:00)
comcast.net IN A 69.252.80.75 30s (00:00:30)
comcast.net IN RRSIG type covered: A (1) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 30 (00:00:30) signature
expiration: 2016-07-05 00:23:38Z signature inception: 2016-06-27 21:18:38Z key tag: 44553 signer's name: comcast.net
signature:
(1024 bits) 3180B34AED6EB2388ED9968C137C3303
5B1A7EA6A9C5AA2030EEC2026A903B26
EF9E6572AA84FBD3422F1852D99F5556
CBB2ED560E976D2D6F9C3B9EC3013039
FDDEA2F9BCFC7F4D53E09DFF26185309
F335896F504F7D7EFE0ADE21082F6688
13F4CE1BF62ACF0CD48911CF82DF79DA
5A0C210B47097F37FC0835D15369AF26 30s (00:00:30)
comcast.net IN MX preference: 5 exchange: mx1.comcast.net 7200s (02:00:00)
comcast.net IN MX preference: 5 exchange: mx2.comcast.net 7200s (02:00:00)
comcast.net IN RRSIG type covered: MX (15) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 7200 (02:00:00) signature
expiration: 2016-07-05 00:23:38Z signature inception: 2016-06-27 21:18:38Z key tag: 44553 signer's name: comcast.net
signature:
(1024 bits) 7C2349A4639DFEE9FFE53C9A2E3919A
10735E461745E339E941144A024AF229
  
```



79178CAC406365DEBFD80DF2C37B6D6F
 F0221135412CE3DABF25290DF4DCDCAD
 46A3E6ADD23DB4DFE66E4ADE198D7E8F
 E6956BE91A1DD85AAECAC5BB0724D24C
 F80B27A3A6AFA35366DF2A80CEFFEFEB
 2A608A767D5E3DB29B37B888943346D2 7200s (02:00:00)
 comcast.net IN NS dns102.comcast.net 7200s (02:00:00)
 comcast.net IN NS dns101.comcast.net 7200s (02:00:00)
 comcast.net IN NS dns103.comcast.net 7200s (02:00:00)
 comcast.net IN NS dns104.comcast.net 7200s (02:00:00)
 comcast.net IN NS dns105.comcast.net 7200s (02:00:00)
 comcast.net IN RRSIG type covered: NS (2) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 7200 (02:00:00) signature
 expiration: 2016-07-05 00:23:38Z signature inception: 2016-06-27 21:18:38Z key tag: 44553 signer's name: comcast.net
 signature:
 (1024 bits) 9EC0F31E2F18BDE9801116AF00D4058F
 F5F260039789F8BC5BE493D3A07345EC
 2396979172E55B88145CC0AA33DC5C9C
 9CAFFD529F37DF2351911382100E6CCA
 B426293CDDDB059C9F5DD185CDAD322A2
 15D9D03696EB9CA6E792F82DD6B5D9EF
 8058AF290EFE6672265F15850F1CF6B4
 D53BD9C5DD93574BA8860E8AF55E84A7 7200s (02:00:00)
 comcast.net IN TXT v=spf1 ip4:96.114.154.128/25 ip4:69.252.207.0/25 include:_spf6.comcast.net include:_spf.mdp.comcast.net ?all
 7200s (02:00:00)
 comcast.net IN RRSIG type covered: TXT (16) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 7200 (02:00:00) signature
 expiration: 2016-07-05 00:23:38Z signature inception: 2016-06-27 21:18:38Z key tag: 44553 signer's name: comcast.net
 signature:
 (1024 bits) 593ABBAE80F2D4FD7DDBB9BD187A9EE5
 420F3730E78F4D5DEA1E570B45B1283C
 686EEB1B34573158D7FE99B8785363F2
 DEA713770691935C0136740939922958
 C2BD1BE02E71157E2F4CCDA9F7E80E3D
 8040EB0F7E7F6DE39B417006333D05BB
 CECC933DE6E3E9D3357A5EDEF60BC79E
 4EB82F1815CE0DB563BE5C13D53A323C 7200s (02:00:00)
 comcast.net IN NSEC next domain name: 4gmobile.comcast.net record types: A NS SOA MX TXT RRSIG NSEC DNSKEY
 3600s (01:00:00)
 comcast.net IN RRSIG type covered: NSEC (47) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 3600 (01:00:00) signature
 expiration: 2016-07-05 00:23:38Z signature inception: 2016-06-27 21:18:38Z key tag: 44553 signer's name: comcast.net
 signature:
 (1024 bits) 742926D80E679BED36738567B4DA8660
 8F7C19336D9DB5FE37EB895977ABB1E7
 AEA80F8DD81971E3097A551DF6E7D45E
 557EAB282B599ADAE39FE88C79B21276
 2E0467A3D2C7B97D1C5F335761AD762C
 990AF63CEA81B9C302D4BE828FBB1B5C
 603BDA025F4297A71AC1D4B40D3E052E
 0AA02BBF950A2C83F43268A43E858E5D 3600s (01:00:00)
 comcast.net IN DNSKEY flags: ZoneKey (256) protocol: 3 algorithm: RSA/SHA-1 (5) public key:
 (1056 bits) 03010001CA97AA33D8252C366DFEFC49
 7CF723676A27CC98507CC103DB63E7D3
 6BC5386CB117903AA8C30556F0722F9C
 C8878AEF6A0CB46EE2C4392A1EECB1F1



75DA4A5E1697D475A8302109DF494861
 1ED85D247B70F917CA36DBF0085118A7
 957D15F56555E71972CEA2C9DE89FE46
 071354117F189DECCE98DEBAE6697E95
 B72D858B 3600s (01:00:00)
 comcast.net IN DNSKEY flags: SecureEntryPoint, ZoneKey (257) protocol: 3 algorithm: RSA/SHA-1 (5) public key:
 (2080 bits) 03010001C753C17B8A204454A0468E1C
 211A7CF0A01D6F03ABC39FB433C3D6C6
 42C02507ED58DF49742982F918506FBA
 14DF4834FDAE1F26F345EFE6E041BC1C
 3F3390AB5A201CEB61921C6DC86E5CA6
 796E2C248F58483131A50C6D230F48F7
 AE3889924DDD0E4CA02AF57C16CC0426
 8F57EFE0966ED7F858A817AA777FD897
 2C9620CAE17BA316CC36EDE5A95E51D9
 B794AE41BD0DD6398C6B31125F060962
 D19771EE6F8B8A4186513D3948024259
 313F179DBDA7A54F984AC583F79481F8
 BE306B28CCD013B3B3A01E253AC25585
 BBC31755595330BA9F8DB0F165AF8C10
 D8DD38A53AFB02F497BB0CE0F7C90960
 726890F343CCE339277D027BE803F162
 BAE8C131 3600s (01:00:00)
 comcast.net IN RRSIG type covered: DNSKEY (48) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 3600 (01:00:00)
 signature expiration: 2016-10-18 21:23:38Z signature inception: 2016-06-20 17:23:38Z key tag: 40909 signer's name:
 comcast.net signature:
 (2048 bits) 336FDBCBA74E9D0D5950E01A3435157B
 8637A8500996E54C9F769EBE7F7739B3
 42B8D1595E054A80AD43D1F4D8A493EE
 F32DA95BD957ADD42C1C1E5DB7B463CA
 6E8184313CDE119686306398C384BD77
 724B665A659B709C691FC8588372031D
 D362D25FDF5336B193D510B6F1E9BA28
 A67569FB3BF0A7A32D36B84BE96FADE7
 B8B1FAA73D14085A46E42C5C29682687
 D32C5729F7A72BA01DDB01AC8DE96963
 28FB42E7ADB3C38C797465782629D299
 69997B123420DDF7DAE46CA0707AAE05
 B1274FBD835000F7A905989685AC5C0E
 87B15C7D0D09B4CA5CA0A94B9F5D3D23
 9271134B64803762B385B149034F856C
 A31C7E8699ED8236AA774C23094E5A38 3600s (01:00:00)
 comcast.net IN RRSIG type covered: DNSKEY (48) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 3600 (01:00:00)
 signature expiration: 2016-07-05 00:23:38Z signature inception: 2016-06-27 21:18:38Z key tag: 44553 signer's name:
 comcast.net signature:
 (1024 bits) 1A1656F5423BCA3ECE007B2A05241D47
 4BC37E9FCE7F833AC69D2345A30887CF
 09D75CB0871A16761BE3C156AEF057B2
 72DCC1089FEBD838EEAAECE069944FCA
 1FA7C9740F778BCF749E4414E86A4B70
 3E90FA771E423958E0E7B273FCAB017C
 FB8BF0F79708247BFB5902FA2F63BE5F
 A3FA8C71045A57826797025B950A9E87 3600s (01:00:00)



comcast.net IN SOA server: dns101.comcast.net email: domregtech@comcastonline.com serial: 2008188833 refresh: 7200
 retry: 3600 expire: 1209600 minimum ttl: 3600 7200s (02:00:00)
 comcast.net IN RRSIG type covered: SOA (6) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 7200 (02:00:00) signature
 expiration: 2016-07-05 00:23:38Z signature inception: 2016-06-27 21:18:38Z key tag: 44553 signer's name: comcast.net
 signature:
 (1024 bits) 7852689A3093F4BF3D6C0F567BAE5D2A
 79799A6A135BBD20292D7B3857C6EB55
 C53D23C38A8748B734EE014A00B137AB
 370402CD8627626E86C3EA76927E93BD
 C7E6EA0844B187C75B798DF31BAB79FE
 AD42217C777A4FE2D9A73BE79E5FFC5FC
 594CE4A70795687FD410F2049E5D5536
 DDEFCFEAE06D7F1F8443E6367CB17875 7200s (02:00:00)
 58.154.91.24.in-addr.arpa IN PTR c-24-91-154-58.hsd1.vt.comcast.net 7200s (02:00:00)
 154.91.24.in-addr.arpa IN NS dns102.comcast.net 7200s (02:00:00)
 154.91.24.in-addr.arpa IN NS dns103.comcast.net 7200s (02:00:00)
 154.91.24.in-addr.arpa IN NS dns104.comcast.net 7200s (02:00:00)
 154.91.24.in-addr.arpa IN NS dns105.comcast.net 7200s (02:00:00)
 154.91.24.in-addr.arpa IN NS dns101.comcast.net 7200s (02:00:00)
 154.91.24.in-addr.arpa IN SOA server: dns101.comcast.net email: dnsadmin@comcast.net serial: 2139 refresh: 7200
 retry: 3600 expire: 604800 minimum ttl: 7200 7200s (02:00:00)

Traceroute

Tracing route to c-24-91-154-58.hsd1.vt.comcast.net [24.91.154.58] ...				hop	rtt	rtt	rtt	ip address	fully qualified
domain name									
1	1	0	0	208.101.16.73	49.10.65d0.ip4.static.sl-reverse.com				
2	0	0	0	66.228.118.153	ae11.dar01.sr01.dal01.networklayer.com				
3	0	0	0	173.192.18.210	ae6.bbr01.eq01.dal03.networklayer.com				
4	0	0	0	75.149.228.33	be-111-pe03.1950stemmons.tx.ibone.comcast.net				
5	3	2	2	68.86.89.249	hu-0-4-0-9-cr02.dallas.tx.ibone.comcast.net				
6	16	17	16	68.86.84.229	be-11724-cr02.denver.co.ibone.comcast.net				
7	29	29	29	68.86.85.169	be-10517-cr02.350ecermak.il.ibone.comcast.net				
8	58	58	58	68.86.91.6	be-7922-ar01.woburn.ma.boston.comcast.net				
9	62	62	62	162.151.113.14					
10	61	64	61	68.85.142.62	te-1-0-0-ten02.bennington.vt.boston.comcast.net				
11	*	*	*						
12	*	*	*						
13	*	*	*						
14	*	*	*						

Trace aborted

=====

Country: US
 Region: VT
 City: Bennington
 Postal Code: 05201
 Latitude: 42.8626
 Longitude: -73.0998
 Metropolitan Code: Albany-Schenectady-Troy
 ISP: Comcast Cable
 Organization: Comcast Cable



=====

Country: US
Region: VT
City: Bennington
Postal Code: 05201
Latitude: 42.8781345
Longitude: -73.1967741
Area: 12.507 sq. km. (4.829 sq. miles)

=====

VPN: Vermont Office of Attorney General Criminal Division

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:53 UTC

This concludes Section D

This concludes CyberTipline Report 11614028



CyberTipline Report 11751258

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 05-23-2016 19:15:43 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*

Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Section C: Additional Information Provided by NCMEC	4
NCMEC Note #1	4
NCMEC Note #2	4
NCMEC Note #3	4
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 01-01-0001 00:00:00 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
Peer to Peer Filenames: tmp36DA.jpg

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename:	tmp36DA.jpg
Was File Reviewed by Company?	Yes
Child Pornography Categorization by ESP: (See Section B for further explanation)	A2
Original Binary Hash of File (PhotoDNA):	52,88,65,17,44,87,105,36,125,8,52,22,84,43,62,22,66,93,56,109,16,134,7 0,38,87,78,27,87,50,90,86,126,99,23,22,82,120,10,31,40,62,91,110,37,24 ,110,59,39,21,24,11,95,30,22,2,118,110,6,12,79,234,6,56,52,51,136,64,5 6,37,56,60,28,10,60,72,15,27,12,122,26,167,23,134,28,239,50,122,57,24, 120,14,85,28,31,14,52,50,25,13,62,85,10,64,112,234,64,190,137,100,96, 57,130,52,184,3,125,105,24,17,72,38,12,0,88,63,13,3,121,140,11,11,232, 46,58,1,205,29,114,17,150,97,10,11,125
Original URL Where File was Located:	D:\local\Temp\tmp36DA.jpg

**Additional Information:****Where to serve legal process in Criminal Matters**

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other Online Services:

FAX: (425) 708-0096 Microsoft Corporation
Attn: Online Services Custodian of Records
One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A2: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-RHS 06-27-2016 19:42:47 UTC

Microsoft provided the following reported user information:

Screen Name: vt151232
IP Address: 24.91.154.58

NCMEC Note #2

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #3

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.



For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 11751258



CyberTipline Report 13202385

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 07-18-2016 16:26:52 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6
Homeland Security Investigations	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 07-18-2016 10:32:48 UTC

Peer to Peer

Peer-to-Peer Client: Skype
IP_ADDRESS: 64.223.160.42
Peer to Peer Filenames: tmpF584.jpg

User or Person Being Reported

Screen/User Name: cjvt1412345,842e0d79f4392b0b
IP Address: 64.223.160.42
Device ID (Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmpF584.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A1
(See Section B for further explanation)



Original Binary Hash of File (PhotoDNA): 0,42,0,38,0,93,4,54,34,39,32,59,101,21,26,123,83,31,20,92,184,0,12,23,0,68,29,75,0,56,4,72,39,13,22,54,52,2,25,37,113,1,52,11,175,1,22,26,0,15,9,103,12,1,103,52,42,40,10,58,48,82,10,34,74,115,8,9,75,45,47,1,170,0,1,24,29,36,44,120,111,12,119,63,224,18,39,94,128,33,43,64,35,83,6,28,11,57,11,86,124,78,147,36,192,20,75,157,154,59,13,93,169,67,60,34,248,35,31,4,247,1,6,43,239,1,48,31,183,7,15,50,139,8,35,14,246,5,40,5,234,13,25,3,153,11

Original URL Where File was Located: D:\local\Temp\tmpF584.jpg

Additional Information: Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other Online Services:
 FAX: (425) 708-0096 Microsoft Corporation
 Attn: Online Services Custodian of Records
 One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS
 Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT
 Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	64.223.160.42		
Device ID (Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
64.223.160.42	US	VT	Readsboro	Albany-Schenectady-Troy	05350		42.7992 / -72.9717	Fairpoint Communications/ Fairpoint Communications

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



64.223.160.42	US	VT	Readsboro	Albany-Schenectady-Troy	05350	42.7992/72.9717	- Fairpoint Communications/Fairpoint Communications
---------------	----	----	-----------	-------------------------	-------	-----------------	-----------------------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	08-11-2016 18:04:17 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	13202393, 13202385

NCMEC Note #1

ECD-JPR 08-11-2016 18:04:17 UTC

CT/TA Search results for: cjvt1412345

13202385

13202393

CT/TA Search results for: 842e0d79f4392b0b

13202385

13202393

CT/TA Search results for: 64.223.160.42

13202385

13202393

=====

VPN: VT ICAC

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agencies listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 08-11-2016 18:04:17 UTC

Homeland Security Investigations

Investigator:

Title:	Caitlin Moynihan
City/State:	VT
Phone Number:	8026605016
Email Address:	caitlin.e.moynihan@ice.dhs.gov

Time/Date was made available: 09-27-2016 15:28:16 UTC

This concludes Section D

This concludes CyberTipline Report 13202385



CyberTipline Report 13202393

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 07-18-2016 16:26:56 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*

Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6
Homeland Security Investigations	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 07-18-2016 10:22:51 UTC

Peer to Peer

Peer-to-Peer Client: Skype
IP_ADDRESS: 64.223.160.42
Peer to Peer Filenames: tmp396.jpg

User or Person Being Reported

Screen/User Name: cjvt1412345,842e0d79f4392b0b
IP Address: 64.223.160.42
Device ID (Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp396.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A2
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

11,53,0,126,22,97,15,101,11,255,27,108,33,212,51,28,107,30,198,1,23,3
 2,174,31,8,80,0,171,53,50,3,223,18,189,23,107,53,130,153,14,198,30,11
 2,24,21,33,132,52,2,87,15,72,92,53,37,76,54,114,45,58,77,95,56,40,108,
 70,51,126,32,37,25,90,27,145,43,74,126,41,71,104,66,120,45,50,59,101,
 40,45,89,74,86,67,27,63,26,42,28,181,90,78,97,67,70,97,69,72,41,84,47,
 64,41,62,63,65,51,78,13,128,9,112,44,128,47,109,83,59,38,131,75,44,45,
 66,37,57,52,26,15,103,33,75,0,120,1,98

Original URL Where File was Located:

D:\local\Temp\tmp396.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
 Online Services:

FAX: (425) 708-0096 Microsoft Corporation

Attn: Online Services Custodian of Records

One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	64.223.160.42		
Device ID (Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A2: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
64.223.160.42	US	VT	Readsboro	Albany-Schenectady-Troy	05350		42.7992 / -72.9717	Fairpoint Communications/ Fairpoint Communications

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



64.223.160.42	US	VT	Readsboro	Albany-Schenectady-Troy	05350	42.7992/72.9717	- Fairpoint Communications/Fairpoint Communications
---------------	----	----	-----------	-------------------------	-------	-----------------	-----------------------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	08-11-2016 18:04:23 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	13202385

NCMEC Note #1

ECD-JPR 08-11-2016 18:04:23 UTC

There are multiple reports on this target. Please see CT #13202385 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agencies listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 08-11-2016 18:04:23 UTC

Homeland Security Investigations

Investigator:

Title:	Caitlin Moynihan
City/State:	VT
Phone Number:	8026605016
Email Address:	caitlin.e.moynihan@ice.dhs.gov

Time/Date was made available: 09-27-2016 15:28:13 UTC

This concludes Section D

This concludes CyberTipline Report 13202393



CyberTipline Report 13281876

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 07-22-2016 17:52:34 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6
Homeland Security Investigations	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 07-22-2016 00:43:25 UTC

Peer to Peer

Peer-to-Peer Client: Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmpBFE1.jpg

User or Person Being Reported

Screen/User Name: cjvt12345,acc278424f43a9e8
IP Address: 24.91.154.58
Device ID (Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmpBFE1.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A1
(See Section B for further explanation)



Original Binary Hash of File (PhotoDNA): 0,42,0,38,0,93,4,54,34,39,32,59,101,21,26,123,83,31,20,92,184,0,12,23,0,68,29,75,0,56,4,72,39,13,22,54,52,2,25,37,113,1,52,11,175,1,22,26,0,15,9,103,12,1,103,52,42,40,10,58,48,82,10,34,74,115,8,9,75,45,47,1,170,0,1,24,29,36,44,120,111,12,119,63,224,18,39,94,128,33,43,64,35,83,6,28,11,57,11,86,124,78,147,36,192,20,75,157,154,59,13,93,169,67,60,34,248,35,31,4,247,1,6,43,239,1,48,31,183,7,15,50,139,8,35,14,246,5,40,5,234,13,25,3,153,11

Original URL Where File was Located: D:\local\Temp\tmpBFE1.jpg

Additional Information: Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other Online Services:
 FAX: (425) 708-0096 Microsoft Corporation
 Attn: Online Services Custodian of Records
 One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS
 Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT
 Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201	42.8626/73.0998	-	Comcast Cable/Comcast Cable
--------------	----	----	------------	-------------------------	-------	-----------------	---	-----------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	08-17-2016 13:01:41 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	13711825, 13712405, 13281882, 13337689, 13281881, 13712450, 13711685, 13711686, 13712041, 13337682, 13712042, 13712170, 13395344, 13712333, 13337686, 13674862, 13711695

NCMEC Note #1

ECD-JPR 08-17-2016 12:55:44 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

NCMEC Note #2

ECD-JPR 08-17-2016 13:01:43 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agencies listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 09-26-2016 17:01:32 UTC

Homeland Security Investigations

Investigator:

Title:	Caitlin Moynihan
City/State:	VT
Phone Number:	8026605016
Email Address:	caitlin.e.moynihan@ice.dhs.gov

Time/Date was made available: 09-26-2016 17:03:50 UTC

This concludes Section D

This concludes CyberTipline Report 13281876



CyberTipline Report 13281881

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 07-22-2016 17:52:34 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6
Homeland Security Investigations	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 07-22-2016 00:31:41 UTC

Peer to Peer

Peer-to-Peer Client: Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmpBF42.jpg

User or Person Being Reported

Screen/User Name: cjvt12345,acc278424f43a9e8
IP Address: 24.91.154.58
Device ID (Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmpBF42.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A1
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

23,42,8,61,113,41,33,57,122,84,34,82,74,26,41,55,17,37,26,28,31,42,58,
 35,49,122,75,53,57,38,28,67,142,44,39,70,87,11,36,47,80,9,68,16,65,42,
 99,10,54,216,76,14,46,57,87,4,116,45,46,61,134,4,31,83,51,16,17,68,111
 ,3,9,64,77,188,76,5,127,128,117,52,80,148,112,70,110,13,55,57,77,31,33
 ,86,173,4,44,28,81,221,62,51,118,208,53,160,170,100,99,108,91,29,73,2
 8,103,62,103,21,147,24,46,42,102,95,48,112,70,102,219,56,99,110,58,53
 ,166,6,23,13,69,45,114,24,33,176,28,166

Original URL Where File was Located:

D:\local\Temp\tmpBF42.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
 Online Services:

FAX: (425) 708-0096 Microsoft Corporation
 Attn: Online Services Custodian of Records
 One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201	42.8626/73.0998	-	Comcast Cable/Comcast Cable
--------------	----	----	------------	-------------------------	-------	-----------------	---	-----------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	08-17-2016 13:01:41 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	13711825, 13712405, 13281882, 13337689, 13712450, 13711685, 13711686, 13712041, 13337682, 13712042, 13712170, 13395344, 13712333, 13337686, 13281876, 13674862, 13711695

NCMEC Note #1

ECD-JPR 08-17-2016 12:55:44 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

NCMEC Note #2

ECD-JPR 08-17-2016 13:01:43 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agencies listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 09-26-2016 17:01:35 UTC

Homeland Security Investigations

Investigator:

Title:	Caitlin Moynihan
City/State:	VT
Phone Number:	8026605016
Email Address:	caitlin.e.moynihan@ice.dhs.gov

Time/Date was made available: 09-26-2016 17:04:00 UTC

This concludes Section D

This concludes CyberTipline Report 13281881



CyberTipline Report 13281882

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 07-22-2016 17:52:34 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
Section D: Law Enforcement Contact Information	8
Vermont Office of Attorney General	8
Homeland Security Investigations	8



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 07-22-2016 00:39:18 UTC

Peer to Peer

Peer-to-Peer Client: Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmpBF92.jpg

User or Person Being Reported

Screen/User Name: cjvt12345,acc278424f43a9e8
IP Address: 24.91.154.58
Device ID (Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmpBF92.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A1
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

67,54,31,44,53,130,75,57,76,57,171,18,12,88,230,4,54,37,211,29,170,16,
 224,20,58,65,114,7,105,81,221,8,113,34,243,16,25,66,196,46,47,69,217,
 59,78,137,115,143,48,47,103,6,103,36,73,22,26,87,39,53,12,89,48,71,55,
 111,47,114,133,99,152,80,93,16,20,156,28,34,15,129,28,50,17,81,9,127,
 36,121,64,71,35,139,94,48,48,162,43,1,16,72,79,1,27,66,68,27,38,28,4,1
 67,71,23,6,62,34,31,14,16,6,52,50,0,38,0,86,0,69,0,68,22,100,3,3,141,73,
 4,0,90,51,0,0,16,31,0

Original URL Where File was Located:

D:\local\Temp\tmpBF92.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
 Online Services:

FAX: (425) 708-0096 Microsoft Corporation

Attn: Online Services Custodian of Records

One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201	42.8626/73.0998	-	Comcast Cable/Comcast Cable
--------------	----	----	------------	-------------------------	-------	-----------------	---	-----------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	08-17-2016 12:55:00 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	13711825, 13712405, 13281882, 13337689, 13281881, 13712450, 13711685, 13711686, 13712041, 13337682, 13712042, 13712170, 13395344, 13712333, 13337686, 13281876, 13674862, 13711695

NCMEC Note #1

ECD-JPR 08-17-2016 13:02:18 UTC

CT/TA Search results for: *cjvt12345*

13281876

13281881

13281882

CT/TA Search results for: acc278424f43a9e8

13281876

13281881

13281882

CT/TA Search results for: 24.91.154.58

13281876

13281881

13281882

13337682

13337686

13337689

13395344

13674862

13711685

13711686

13711695

13711825

13712041

13712042

13712170

13712333

13712405

13712450

12766078 VT

12765579 VT

12765571 VT



12651701 VT
12651697 VT
12651690 VT
12627589 VT
12627584 VT
12627552 VT
12527760 VT
12527752 VT
12526159 VT
12526157 VT
12526156 VT
12526155 VT
12526153 VT
12526152 VT
12526151 VT
12526150 VT
12526149 VT
12469964 VT
12469962 VT
12469960 VT
12469951 VT
12468566 VT
12468560 VT
12415755 VT
12415578 VT
12415511 VT
12415510 VT
12116763 VT
12114081 VT
51 to 62
12114080 VT
12114079 VT
12051925 VT
12051516 VT
12050739 VT
12050735 VT
12050728 VT
12045016 VT
11855790 VT
11751259 VT
11751258 VT
11614028 VT

=====

Identifiers from related reports:

CT/TA Search results for: *cjvt123*

13281876
13281881
13281882
13337682
13337686



13337689

CT/TA Search results for: a4ddfb1a1bf6f05c

13337682

13337686

13337689

CT/TA Search results for: *cjny123*

13395344

CT/TA Search results for: 967718d675b7ef97

13395344

CT/TA Search results for: *ash141234*

13674862

13711685

13711825

CT/TA Search results for: *britt14123*

13711686

13711695

13712041

13712042

13712170

13712450

CT/TA Search results for: *madi141234*

13712333

13712405

CT/TA Search results for: *cjvt12345*

13281876

13281881

13281882

CT/TA Search results for: acc278424f43a9e8

13281876

13281881

13281882

=====

VPN: VT ICAC

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agencies listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 08-17-2016 12:55:40 UTC

Homeland Security Investigations

Investigator:

Title:	Caitlin Moynihan
City/State:	VT
Phone Number:	8026605016
Email Address:	caitlin.e.moynihan@ice.dhs.gov

Time/Date was made available: 09-26-2016 17:06:41 UTC

This concludes Section D

This concludes CyberTipline Report 13281882



CyberTipline Report 13337682

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 07-25-2016 17:03:37 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6
Homeland Security Investigations	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 07-24-2016 23:25:24 UTC

Peer to Peer

Peer-to-Peer Client: Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmpDBA.jpg

User or Person Being Reported

Screen/User Name: cjvt123,a4ddfb1a1bf6f05c
IP Address: 24.91.154.58
Device ID (Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmpDBA.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A2
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

18,13,7,50,23,9,12,18,46,50,14,17,13,79,22,42,92,14,11,55,8,42,7,16,44,
23,49,69,39,43,53,130,20,59,22,236,15,110,26,217,90,23,15,236,46,25,1
9,220,34,31,8,171,8,110,9,216,8,102,46,208,18,32,65,186,90,36,64,167,1
16,34,100,150,1,147,26,50,12,52,7,103,36,34,50,98,39,31,78,46,42,55,76
,85,44,52,21,152,1,193,88,26,1,133,68,45,74,30,30,101,117,51,37,41,9,1
56,21,94,49,27,27,90,10,56,58,16,2,160,180,4,53,55,183,2,93,48,120,15,
11,133,136,6,82,7,171,1

Original URL Where File was Located:

D:\local\Temp\tmpDBA.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
Online Services:

FAX: (425) 708-0096 Microsoft Corporation
Attn: Online Services Custodian of Records
One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A2: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201	42.8626/73.0998	-	Comcast Cable/Comcast Cable
--------------	----	----	------------	-------------------------	-------	-----------------	---	-----------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	08-17-2016 13:01:41 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	13711825, 13712405, 13281882, 13337689, 13281881, 13712450, 13711685, 13711686, 13712041, 13712042, 13712170, 13395344, 13712333, 13337686, 13281876, 13674862, 13711695

NCMEC Note #1

ECD-JPR 08-17-2016 12:55:44 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

NCMEC Note #2

ECD-JPR 08-17-2016 13:01:43 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agencies listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 09-26-2016 17:01:39 UTC

Homeland Security Investigations

Investigator:

Title:	Caitlin Moynihan
City/State:	VT
Phone Number:	8026605016
Email Address:	caitlin.e.moynihan@ice.dhs.gov

Time/Date was made available: 09-26-2016 17:04:10 UTC

This concludes Section D

This concludes CyberTipline Report 13337682



CyberTipline Report 13337686

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 07-25-2016 17:03:47 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*

Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6
Homeland Security Investigations	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 07-25-2016 00:07:10 UTC

Peer to Peer

Peer-to-Peer Client: Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp10C9.jpg

User or Person Being Reported

Screen/User Name: cjvt123,a4ddfb1a1bf6f05c
IP Address: 24.91.154.58
Device ID (Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp10C9.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A1
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

67,54,31,44,53,130,75,57,76,57,171,18,12,88,230,4,54,37,211,29,170,16,
224,20,58,65,114,7,105,81,221,8,113,34,243,16,25,66,196,46,47,69,217,
59,78,137,115,143,48,47,103,6,103,36,73,22,26,87,39,53,12,89,48,71,55,
111,47,114,133,99,152,80,93,16,20,156,28,34,15,129,28,50,17,81,9,127,
36,121,64,71,35,139,94,48,48,162,43,1,16,72,79,1,27,66,68,27,38,28,4,1
67,71,23,6,62,34,31,14,16,6,52,50,0,38,0,86,0,69,0,68,22,100,3,3,141,73,
4,0,90,51,0,0,16,31,0

Original URL Where File was Located:

D:\local\Temp\tmp10C9.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
Online Services:

FAX: (425) 708-0096 Microsoft Corporation
Attn: Online Services Custodian of Records
One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201	42.8626/73.0998	-	Comcast Cable/Comcast Cable
--------------	----	----	------------	-------------------------	-------	-----------------	---	-----------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	08-17-2016 13:01:41 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	13711825, 13712405, 13281882, 13337689, 13281881, 13712450, 13711685, 13711686, 13712041, 13337682, 13712042, 13712170, 13395344, 13712333, 13281876, 13674862, 13711695

NCMEC Note #1

ECD-JPR 08-17-2016 12:55:44 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

NCMEC Note #2

ECD-JPR 08-17-2016 13:01:43 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agencies listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 09-26-2016 17:01:42 UTC

Homeland Security Investigations

Investigator:

Title:	Caitlin Moynihan
City/State:	VT
Phone Number:	8026605016
Email Address:	caitlin.e.moynihan@ice.dhs.gov

Time/Date was made available: 09-26-2016 17:04:20 UTC

This concludes Section D

This concludes CyberTipline Report 13337686



CyberTipline Report 13337689

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 07-25-2016 17:03:47 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6
Homeland Security Investigations	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 07-24-2016 23:45:07 UTC

Peer to Peer

Peer-to-Peer Client: Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp1185.jpg

User or Person Being Reported

Screen/User Name: cjvt123,a4ddfb1a1bf6f05c
IP Address: 24.91.154.58
Device ID (Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp1185.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A1
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

15,23,0,115,6,29,0,172,17,14,0,228,13,36,0,160,37,2,4,60,68,0,10,57,9,3
 2,68,32,0,72,53,59,3,22,12,87,24,0,9,85,38,2,19,75,33,5,50,73,3,33,157,0
 ,1,140,206,2,26,66,220,7,45,23,235,7,105,9,222,16,58,3,176,7,0,58,59,0,
 31,62,92,17,71,97,214,37,69,70,178,99,56,61,119,49,75,3,63,11,6,50,47,
 63,50,30,114,87,51,119,110,86,35,62,100,31,64,29,104,59,54,16,79,104,
 51,26,32,209,59,56,47,252,143,40,80,121,29,47,36,5,25,175,22,116,33,5
 0,36,225

Original URL Where File was Located:

D:\local\Temp\tmp1185.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
 Online Services:

FAX: (425) 708-0096 Microsoft Corporation

Attn: Online Services Custodian of Records

One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201	42.8626/73.0998	-	Comcast Cable/Comcast Cable
--------------	----	----	------------	-------------------------	-------	-----------------	---	-----------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	08-17-2016 13:01:41 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	13711825, 13712405, 13281882, 13281881, 13712450, 13711685, 13711686, 13712041, 13337682, 13712042, 13712170, 13395344, 13712333, 13337686, 13281876, 13674862, 13711695

NCMEC Note #1

ECD-JPR 08-17-2016 12:55:44 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

NCMEC Note #2

ECD-JPR 08-17-2016 13:01:43 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agencies listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 09-26-2016 17:01:45 UTC

Homeland Security Investigations

Investigator:

Title:	Caitlin Moynihan
City/State:	VT
Phone Number:	8026605016
Email Address:	caitlin.e.moynihan@ice.dhs.gov

Time/Date was made available: 09-26-2016 17:04:31 UTC

This concludes Section D

This concludes CyberTipline Report 13337689



CyberTipline Report 13395344

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 07-28-2016 16:05:34 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6
Homeland Security Investigations	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 07-27-2016 23:58:11 UTC

Peer to Peer

Peer-to-Peer Client: Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmpE89D.jpg

User or Person Being Reported

Screen/User Name: cjny123,967718d675b7ef97
IP Address: 24.91.154.58
Device ID (Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmpE89D.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A1
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

9,113,9,108,28,85,54,82,46,33,50,154,82,2,8,201,38,51,12,222,6,80,8,20
 3,42,18,3,224,29,114,12,179,44,93,43,156,77,38,24,191,32,33,0,215,3,47
 ,0,135,22,19,3,113,41,37,0,148,114,74,24,107,48,122,41,60,38,26,5,104,
 65,9,15,42,1,103,114,15,18,50,65,66,167,25,40,54,84,160,90,23,60,40,97
 ,15,134,9,106,13,14,108,177,47,3,109,239,23,102,41,152,22,87,90,74,78,
 54,48,116,83,42,68,44,121,29,28,19,111,7,46,41,138,15,65,48,114,14,49,
 8,100,13,18,7,77,16,25,21,39

Original URL Where File was Located:

D:\local\Temp\tmpE89D.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
 Online Services:

FAX: (425) 708-0096 Microsoft Corporation

Attn: Online Services Custodian of Records

One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201	42.8626/73.0998	-	Comcast Cable/Comcast Cable
--------------	----	----	------------	-------------------------	-------	-----------------	---	-----------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	08-17-2016 13:01:41 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	13711825, 13712405, 13281882, 13337689, 13281881, 13712450, 13711685, 13711686, 13712041, 13337682, 13712042, 13712170, 13712333, 13337686, 13281876, 13674862, 13711695

NCMEC Note #1

ECD-JPR 08-17-2016 12:55:44 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

NCMEC Note #2

ECD-JPR 08-17-2016 13:01:43 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agencies listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 09-26-2016 17:01:49 UTC

Homeland Security Investigations

Investigator:

Title:	Caitlin Moynihan
City/State:	VT
Phone Number:	8026605016
Email Address:	caitlin.e.moynihan@ice.dhs.gov

Time/Date was made available: 09-26-2016 17:04:41 UTC

This concludes Section D

This concludes CyberTipline Report 13395344



CyberTipline Report 13674862

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 08-10-2016 23:00:24 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*

Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6
Homeland Security Investigations	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 08-10-2016 01:38:49 UTC

Peer to Peer

Peer-to-Peer Client: Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmpBDF9.jpg
Additional Information: DocumentId: 0-eus-d3-5d80ab5fd5988f6121b1f95e0d0c6cb3
Please provide ScreenName and DocumentId when requesting more information from Microsoft.

User or Person Being Reported

Screen/User Name: ash141234
IP Address: 24.91.154.58
Device ID (Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmpBDF9.jpg
Was File Reviewed by Company? Yes



Child Pornography Categorization by ESP:
(See Section B for further explanation)

B2

Original Binary Hash of File (PhotoDNA):

133,7,45,29,47,133,14,178,69,73,19,159,96,54,83,31,8,95,96,3,20,6,52,0,88,15,24,9,35,155,109,45,125,56,129,33,129,39,51,29,40,107,104,22,23,43,72,10,97,21,32,24,75,102,66,50,57,106,46,70,107,92,6,145,85,95,12,177,46,53,29,103,80,57,24,187,34,90,12,243,46,99,40,138,74,76,57,94,85,40,76,93,188,9,159,23,3,69,118,73,54,17,100,72,104,27,84,47,70,68,91,44,194,24,154,59,106,9,98,19,67,44,111,84,15,75,135,86,51,52,42,115,64,36,36,124,143,27,31,107,175,0,37,40

Original URL Where File was Located:

D:\local\Temp\tmpBDF9.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other Online Services:

FAX: (425) 708-0096 Microsoft Corporation

Attn: Online Services Custodian of Records

One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

B2: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	---------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	08-17-2016 13:01:41 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	13711825, 13712405, 13281882, 13337689, 13281881, 13712450, 13711685, 13711686, 13712041, 13337682, 13712042, 13712170, 13395344, 13712333, 13337686, 13281876, 13711695

NCMEC Note #1

ECD-JPR 08-17-2016 12:55:44 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

NCMEC Note #2

ECD-JPR 08-17-2016 13:01:43 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agencies listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 09-26-2016 17:01:53 UTC

Homeland Security Investigations

Investigator:

Title:	Caitlin Moynihan
City/State:	VT
Phone Number:	8026605016
Email Address:	caitlin.e.moynihan@ice.dhs.gov

Time/Date was made available: 09-26-2016 17:04:52 UTC

This concludes Section D

This concludes CyberTipline Report 13674862



CyberTipline Report 13711685

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 08-12-2016 16:00:36 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6
Homeland Security Investigations	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 08-10-2016 01:22:09 UTC

Peer to Peer

Peer-to-Peer Client: Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp27C8.jpg
Additional Information: DocumentId: 0-eus-d1-493163cfe33121d700ead8475c0b414a
Please provide ScreenName and DocumentId when requesting more information from Microsoft.

User or Person Being Reported

Screen/User Name: ash141234
IP Address: 24.91.154.58
Device ID (Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp27C8.jpg
Was File Reviewed by Company? Yes



Child Pornography Categorization by ESP:
(See Section B for further explanation)

A1

Original Binary Hash of File (PhotoDNA):

67,54,31,44,53,130,75,57,76,57,171,18,12,88,230,4,54,37,211,29,170,16,
224,20,58,65,114,7,105,81,221,8,113,34,243,16,25,66,196,46,47,69,217,
59,78,137,115,143,48,47,103,6,103,36,73,22,26,87,39,53,12,89,48,71,55,
111,47,114,133,99,152,80,93,16,20,156,28,34,15,129,28,50,17,81,9,127,
36,121,64,71,35,139,94,48,48,162,43,1,16,72,79,1,27,66,68,27,38,28,4,1
67,71,23,6,62,34,31,14,16,6,52,50,0,38,0,86,0,69,0,68,22,100,3,3,141,73,
4,0,90,51,0,0,16,31,0

Original URL Where File was Located:

D:\local\Temp\tmp27C8.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
Online Services:

FAX: (425) 708-0096 Microsoft Corporation

Attn: Online Services Custodian of Records

One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	08-17-2016 13:01:41 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	13711825, 13712405, 13281882, 13337689, 13281881, 13712450, 13711686, 13712041, 13337682, 13712042, 13712170, 13395344, 13712333, 13337686, 13281876, 13674862, 13711695

NCMEC Note #1

ECD-JPR 08-17-2016 12:55:44 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

NCMEC Note #2

ECD-JPR 08-17-2016 13:01:43 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agencies listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 09-26-2016 17:01:58 UTC

Homeland Security Investigations

Investigator:

Title:	Caitlin Moynihan
City/State:	VT
Phone Number:	8026605016
Email Address:	caitlin.e.moynihan@ice.dhs.gov

Time/Date was made available: 09-26-2016 17:05:02 UTC

This concludes Section D

This concludes CyberTipline Report 13711685



CyberTipline Report 13711686

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 08-12-2016 16:00:37 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6
Homeland Security Investigations	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 08-09-2016 00:24:06 UTC

Peer to Peer

Peer-to-Peer Client: Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp2A6A.jpg
Additional Information: DocumentId: 0-eus-d1-13b96a85d55d9144914836ff72e5744e
Please provide ScreenName and DocumentId when requesting more information from Microsoft.

User or Person Being Reported

Screen/User Name: britt14123
IP Address: 24.91.154.58
Device ID (Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp2A6A.jpg
Was File Reviewed by Company? Yes



Child Pornography Categorization by ESP:
(See Section B for further explanation)

A1

Original Binary Hash of File (PhotoDNA):

0,33,35,0,54,2,26,5,78,68,7,34,70,25,2,59,79,5,19,39,101,31,80,65,3,50,4
5,0,37,2,55,2,64,84,52,7,66,55,25,31,137,5,16,46,75,88,60,77,5,122,45,3
4,43,10,15,33,108,63,101,24,31,100,133,16,109,17,32,58,96,34,78,122,3,
147,60,64,162,17,41,43,255,152,212,20,19,255,76,55,26,48,7,104,59,3,0,
102,16,189,131,92,154,57,69,48,255,158,32,178,9,255,68,109,16,84,46,3
4,66,3,6,45,40,31,87,75,67,87,67,45,155,120,4,224,22,95,2,159,19,43,40,
22,55,14,60,2

Original URL Where File was Located:

D:\local\Temp\tmp2A6A.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
Online Services:

FAX: (425) 708-0096 Microsoft Corporation

Attn: Online Services Custodian of Records

One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	08-17-2016 13:01:41 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	13711825, 13712405, 13281882, 13337689, 13281881, 13712450, 13711685, 13712041, 13337682, 13712042, 13712170, 13395344, 13712333, 13337686, 13281876, 13674862, 13711695

NCMEC Note #1

ECD-JPR 08-17-2016 12:55:44 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

NCMEC Note #2

ECD-JPR 08-17-2016 13:01:43 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agencies listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 09-26-2016 17:02:02 UTC

Homeland Security Investigations

Investigator:

Title:	Caitlin Moynihan
City/State:	VT
Phone Number:	8026605016
Email Address:	caitlin.e.moynihan@ice.dhs.gov

Time/Date was made available: 09-26-2016 17:05:13 UTC

This concludes Section D

This concludes CyberTipline Report 13711686



CyberTipline Report 13711695

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 08-12-2016 16:00:39 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*

Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6
Homeland Security Investigations	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 08-08-2016 03:23:39 UTC

Peer to Peer

Peer-to-Peer Client: Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp32F8.jpg
Additional Information: DocumentId: 0-eus-d3-2e55f1015bfed1b3ecadcd613dfef146
Please provide ScreenName and DocumentId when requesting more information from Microsoft.

User or Person Being Reported

Screen/User Name: britt14123
IP Address: 24.91.154.58
Device ID (Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp32F8.jpg
Was File Reviewed by Company? Yes



Child Pornography Categorization by ESP:
(See Section B for further explanation)

A1

Original Binary Hash of File (PhotoDNA):

56,147,64,26,144,68,65,16,84,52,94,94,103,24,63,151,38,140,57,70,94,7
5,42,10,112,92,47,202,92,126,30,216,60,101,9,255,151,29,37,233,100,10
1,32,255,75,68,16,162,13,8,17,30,14,37,20,54,38,53,73,24,127,38,127,84
,45,103,87,100,58,21,33,84,0,23,21,0,12,16,26,5,104,5,104,3,106,85,147,
16,8,104,58,13,82,8,65,1,0,34,71,0,39,8,89,0,160,0,105,1,109,128,125,36
,21,151,77,14,107,0,75,0,32,45,101,17,38,18,192,0,91,1,118,0,55,112,68,
22,25,91,59,8,92,0,55,0

Original URL Where File was Located:

D:\local\Temp\tmp32F8.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
Online Services:

FAX: (425) 708-0096 Microsoft Corporation

Attn: Online Services Custodian of Records

One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	08-17-2016 13:01:41 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	13711825, 13712405, 13281882, 13337689, 13281881, 13712450, 13711685, 13711686, 13712041, 13337682, 13712042, 13712170, 13395344, 13712333, 13337686, 13281876, 13674862

NCMEC Note #1

ECD-JPR 08-17-2016 12:55:44 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

NCMEC Note #2

ECD-JPR 08-17-2016 13:01:43 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agencies listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 09-26-2016 17:02:06 UTC

Homeland Security Investigations

Investigator:

Title:	Caitlin Moynihan
City/State:	VT
Phone Number:	8026605016
Email Address:	caitlin.e.moynihan@ice.dhs.gov

Time/Date was made available: 09-26-2016 17:05:23 UTC

This concludes Section D

This concludes CyberTipline Report 13711695



CyberTipline Report 13711825

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 08-12-2016 16:01:27 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6
Homeland Security Investigations	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 08-10-2016 01:18:31 UTC

Peer to Peer

Peer-to-Peer Client: Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmpEBE5.jpg
Additional Information: DocumentId: 0-eus-d3-8c7af233ee48726871607c1f3a778bf3
Please provide ScreenName and DocumentId when requesting more information from Microsoft.

User or Person Being Reported

Screen/User Name: ash141234
IP Address: 24.91.154.58
Device ID (Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmpEBE5.jpg
Was File Reviewed by Company? Yes



Child Pornography Categorization by ESP:
(See Section B for further explanation)

A1

Original Binary Hash of File (PhotoDNA):

18,13,7,50,23,9,12,18,46,50,14,17,13,79,22,42,92,14,11,55,8,42,7,16,44,
23,49,69,39,43,53,130,20,59,22,236,15,110,26,217,90,23,15,236,46,25,1
9,220,34,31,8,171,8,110,9,216,8,102,46,208,18,32,65,186,90,36,64,167,1
16,34,100,150,1,147,26,50,12,52,7,103,36,34,50,98,39,31,78,46,42,55,76
,85,44,52,21,152,1,193,88,26,1,133,68,45,74,30,30,101,117,51,37,41,9,1
56,21,94,49,27,27,90,10,56,58,16,2,160,180,4,53,55,183,2,93,48,120,15,
11,133,136,6,82,7,171,1

Original URL Where File was Located:

D:\local\Temp\tmpEBE5.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
Online Services:

FAX: (425) 708-0096 Microsoft Corporation

Attn: Online Services Custodian of Records

One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	08-17-2016 13:01:41 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	13712405, 13281882, 13337689, 13281881, 13712450, 13711685, 13711686, 13712041, 13337682, 13712042, 13712170, 13395344, 13712333, 13337686, 13281876, 13674862, 13711695

NCMEC Note #1

ECD-JPR 08-17-2016 12:55:44 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

NCMEC Note #2

ECD-JPR 08-17-2016 13:01:43 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agencies listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 09-26-2016 17:02:10 UTC

Homeland Security Investigations

Investigator:

Title:	Caitlin Moynihan
City/State:	VT
Phone Number:	8026605016
Email Address:	caitlin.e.moynihan@ice.dhs.gov

Time/Date was made available: 09-26-2016 17:05:34 UTC

This concludes Section D

This concludes CyberTipline Report 13711825



CyberTipline Report 13712041

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 08-12-2016 16:02:49 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6
Homeland Security Investigations	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 08-08-2016 03:11:53 UTC

Peer to Peer

Peer-to-Peer Client: Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp32DA.jpg
Additional Information: DocumentId: 0-eus-d1-022017cb5f5c70e0d2ef3117a5257885
Please provide ScreenName and DocumentId when requesting more information from Microsoft.

User or Person Being Reported

Screen/User Name: britt14123
IP Address: 24.91.154.58
Device ID (Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp32DA.jpg
Was File Reviewed by Company? Yes



Child Pornography Categorization by ESP:
(See Section B for further explanation)

A1

Original Binary Hash of File (PhotoDNA):

67,54,31,44,53,130,75,57,76,57,171,18,12,88,230,4,54,37,211,29,170,16,
224,20,58,65,114,7,105,81,221,8,113,34,243,16,25,66,196,46,47,69,217,
59,78,137,115,143,48,47,103,6,103,36,73,22,26,87,39,53,12,89,48,71,55,
111,47,114,133,99,152,80,93,16,20,156,28,34,15,129,28,50,17,81,9,127,
36,121,64,71,35,139,94,48,48,162,43,1,16,72,79,1,27,66,68,27,38,28,4,1
67,71,23,6,62,34,31,14,16,6,52,50,0,38,0,86,0,69,0,68,22,100,3,3,141,73,
4,0,90,51,0,0,16,31,0

Original URL Where File was Located:

D:\local\Temp\tmp32DA.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
Online Services:

FAX: (425) 708-0096 Microsoft Corporation

Attn: Online Services Custodian of Records

One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	08-17-2016 13:01:41 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	13711825, 13712405, 13281882, 13337689, 13281881, 13712450, 13711685, 13711686, 13337682, 13712042, 13712170, 13395344, 13712333, 13337686, 13281876, 13674862, 13711695

NCMEC Note #1

ECD-JPR 08-17-2016 12:55:44 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

NCMEC Note #2

ECD-JPR 08-17-2016 13:01:43 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agencies listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 09-26-2016 17:02:14 UTC

Homeland Security Investigations

Investigator:

Title:	Caitlin Moynihan
City/State:	VT
Phone Number:	8026605016
Email Address:	caitlin.e.moynihan@ice.dhs.gov

Time/Date was made available: 09-26-2016 17:05:46 UTC

This concludes Section D

This concludes CyberTipline Report 13712041



CyberTipline Report 13712042

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 08-12-2016 16:02:50 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6
Homeland Security Investigations	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 08-08-2016 03:01:36 UTC

Peer to Peer

Peer-to-Peer Client: Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp3339.jpg
Additional Information: DocumentId: 0-eus-d5-36460338a0a2274fe11c3c8353ecbb77
Please provide ScreenName and DocumentId when requesting more information from Microsoft.

User or Person Being Reported

Screen/User Name: britt14123
IP Address: 24.91.154.58
Device ID (Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp3339.jpg
Was File Reviewed by Company? Yes



Child Pornography Categorization by ESP:
(See Section B for further explanation)

A1

Original Binary Hash of File (PhotoDNA):

0,33,35,0,54,2,26,5,78,68,7,34,70,25,2,59,79,5,19,39,101,31,80,65,3,50,4
5,0,37,2,55,2,64,84,52,7,66,55,25,31,137,5,16,46,75,88,60,77,5,122,45,3
4,43,10,15,33,108,63,101,24,31,100,133,16,109,17,32,58,96,34,78,122,3,
147,60,64,162,17,41,43,255,152,212,20,19,255,76,55,26,48,7,104,59,3,0,
102,16,189,131,92,154,57,69,48,255,158,32,178,9,255,68,109,16,84,46,3
4,66,3,6,45,40,31,87,75,67,87,67,45,155,120,4,224,22,95,2,159,19,43,40,
22,55,14,60,2

Original URL Where File was Located:

D:\local\Temp\tmp3339.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
Online Services:

FAX: (425) 708-0096 Microsoft Corporation

Attn: Online Services Custodian of Records

One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	08-17-2016 13:01:41 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	13711825, 13712405, 13281882, 13337689, 13281881, 13712450, 13711685, 13711686, 13712041, 13337682, 13712170, 13395344, 13712333, 13337686, 13281876, 13674862, 13711695

NCMEC Note #1

ECD-JPR 08-17-2016 12:55:44 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

NCMEC Note #2

ECD-JPR 08-17-2016 13:01:43 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agencies listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 09-26-2016 17:02:19 UTC

Homeland Security Investigations

Investigator:

Title:	Caitlin Moynihan
City/State:	VT
Phone Number:	8026605016
Email Address:	caitlin.e.moynihan@ice.dhs.gov

Time/Date was made available: 09-26-2016 17:05:58 UTC

This concludes Section D

This concludes CyberTipline Report 13712042



CyberTipline Report 13712170

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 08-12-2016 16:03:42 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*

Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6
Homeland Security Investigations	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 08-09-2016 01:04:46 UTC

Peer to Peer

Peer-to-Peer Client: Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmpC2.jpg
Additional Information: DocumentId: 0-eus-d4-cbda4ffd73262a1cfcc4b4ef1e7cabd
Please provide ScreenName and DocumentId when requesting more information from Microsoft.

User or Person Being Reported

Screen/User Name: britt14123
IP Address: 24.91.154.58
Device ID (Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmpC2.jpg
Was File Reviewed by Company? Yes



Child Pornography Categorization by ESP:
(See Section B for further explanation)

A1

Original Binary Hash of File (PhotoDNA):

18,13,7,50,23,9,12,18,46,50,14,17,13,79,22,42,92,14,11,55,8,42,7,16,44,
23,49,69,39,43,53,130,20,59,22,236,15,110,26,217,90,23,15,236,46,25,1
9,220,34,31,8,171,8,110,9,216,8,102,46,208,18,32,65,186,90,36,64,167,1
16,34,100,150,1,147,26,50,12,52,7,103,36,34,50,98,39,31,78,46,42,55,76
,85,44,52,21,152,1,193,88,26,1,133,68,45,74,30,30,101,117,51,37,41,9,1
56,21,94,49,27,27,90,10,56,58,16,2,160,180,4,53,55,183,2,93,48,120,15,
11,133,136,6,82,7,171,1

Original URL Where File was Located:

D:\local\Temp\tmpC2.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
Online Services:

FAX: (425) 708-0096 Microsoft Corporation

Attn: Online Services Custodian of Records

One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	08-17-2016 13:01:41 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	13711825, 13712405, 13281882, 13337689, 13281881, 13712450, 13711685, 13711686, 13712041, 13337682, 13712042, 13395344, 13712333, 13337686, 13281876, 13674862, 13711695

NCMEC Note #1

ECD-JPR 08-17-2016 12:55:44 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

NCMEC Note #2

ECD-JPR 08-17-2016 13:01:43 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agencies listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 09-26-2016 17:02:24 UTC

Homeland Security Investigations

Investigator:

Title:	Caitlin Moynihan
City/State:	VT
Phone Number:	8026605016
Email Address:	caitlin.e.moynihan@ice.dhs.gov

Time/Date was made available: 09-26-2016 17:06:08 UTC

This concludes Section D

This concludes CyberTipline Report 13712170



CyberTipline Report 13712333

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 08-12-2016 16:05:56 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6
Homeland Security Investigations	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 08-10-2016 23:53:31 UTC

Peer to Peer

Peer-to-Peer Client: Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp94F.jpg
Additional Information: DocumentId: 0-eus-d1-6bbe15de6677d399caa55fee9378f875
Please provide ScreenName and DocumentId when requesting more information from Microsoft.

User or Person Being Reported

Screen/User Name: madi141234
IP Address: 24.91.154.58
Device ID (Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp94F.jpg
Was File Reviewed by Company? Yes



Child Pornography Categorization by ESP:
(See Section B for further explanation)

A1

Original Binary Hash of File (PhotoDNA):

18,13,7,50,23,9,12,18,46,50,14,17,13,79,22,42,92,14,11,55,8,42,7,16,44,
23,49,69,39,43,53,130,20,59,22,236,15,110,26,217,90,23,15,236,46,25,1
9,220,34,31,8,171,8,110,9,216,8,102,46,208,18,32,65,186,90,36,64,167,1
16,34,100,150,1,147,26,50,12,52,7,103,36,34,50,98,39,31,78,46,42,55,76
,85,44,52,21,152,1,193,88,26,1,133,68,45,74,30,30,101,117,51,37,41,9,1
56,21,94,49,27,27,90,10,56,58,16,2,160,180,4,53,55,183,2,93,48,120,15,
11,133,136,6,82,7,171,1

Original URL Where File was Located:

D:\local\Temp\tmp94F.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
Online Services:

FAX: (425) 708-0096 Microsoft Corporation

Attn: Online Services Custodian of Records

One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	08-17-2016 13:01:41 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	13711825, 13712405, 13281882, 13337689, 13281881, 13712450, 13711685, 13711686, 13712041, 13337682, 13712042, 13712170, 13395344, 13337686, 13281876, 13674862, 13711695

NCMEC Note #1

ECD-JPR 08-17-2016 12:55:44 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

NCMEC Note #2

ECD-JPR 08-17-2016 13:01:43 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agencies listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 09-26-2016 17:02:28 UTC

Homeland Security Investigations

Investigator:

Title:	Caitlin Moynihan
City/State:	VT
Phone Number:	8026605016
Email Address:	caitlin.e.moynihan@ice.dhs.gov

Time/Date was made available: 09-26-2016 17:06:16 UTC

This concludes Section D

This concludes CyberTipline Report 13712333



CyberTipline Report 13712405

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 08-12-2016 16:08:14 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6
Homeland Security Investigations	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 08-10-2016 23:23:10 UTC

Peer to Peer

Peer-to-Peer Client: Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp26F0.jpg
Additional Information: DocumentId: 0-eus-d1-8b1cd087ff67d19fe34b699374a55d6a
Please provide ScreenName and DocumentId when requesting more information from Microsoft.

User or Person Being Reported

Screen/User Name: madi141234
IP Address: 24.91.154.58
Device ID (Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp26F0.jpg
Was File Reviewed by Company? Yes



Child Pornography Categorization by ESP:
(See Section B for further explanation)

A1

Original Binary Hash of File (PhotoDNA):

18,13,7,50,23,9,12,18,46,50,14,17,13,79,22,42,92,14,11,55,8,42,7,16,44,
23,49,69,39,43,53,130,20,59,22,236,15,110,26,217,90,23,15,236,46,25,1
9,220,34,31,8,171,8,110,9,216,8,102,46,208,18,32,65,186,90,36,64,167,1
16,34,100,150,1,147,26,50,12,52,7,103,36,34,50,98,39,31,78,46,42,55,76
,85,44,52,21,152,1,193,88,26,1,133,68,45,74,30,30,101,117,51,37,41,9,1
56,21,94,49,27,27,90,10,56,58,16,2,160,180,4,53,55,183,2,93,48,120,15,
11,133,136,6,82,7,171,1

Original URL Where File was Located:

D:\local\Temp\tmp26F0.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
Online Services:

FAX: (425) 708-0096 Microsoft Corporation

Attn: Online Services Custodian of Records

One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	- Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	-----------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	08-17-2016 13:01:41 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	13711825, 13281882, 13337689, 13281881, 13712450, 13711685, 13711686, 13712041, 13337682, 13712042, 13712170, 13395344, 13712333, 13337686, 13281876, 13674862, 13711695

NCMEC Note #1

ECD-JPR 08-17-2016 12:55:44 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

NCMEC Note #2

ECD-JPR 08-17-2016 13:01:43 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agencies listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 09-26-2016 17:02:33 UTC

Homeland Security Investigations

Investigator:

Title:	Caitlin Moynihan
City/State:	VT
Phone Number:	8026605016
Email Address:	caitlin.e.moynihan@ice.dhs.gov

Time/Date was made available: 09-26-2016 17:06:26 UTC

This concludes Section D

This concludes CyberTipline Report 13712405



CyberTipline Report 13712450

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 08-12-2016 16:10:34 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6
Homeland Security Investigations	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 08-09-2016 00:30:17 UTC

Peer to Peer

Peer-to-Peer Client: Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp2CFD.jpg
Additional Information: DocumentId: 0-eus-d3-e1a39e7d211a003118d58e4274178408
Please provide ScreenName and DocumentId when requesting more information from Microsoft.

User or Person Being Reported

Screen/User Name: britt14123
IP Address: 24.91.154.58
Device ID (Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp2CFD.jpg
Was File Reviewed by Company? Yes



Child Pornography Categorization by ESP:
(See Section B for further explanation)

A1

Original Binary Hash of File (PhotoDNA):

18,13,7,50,23,9,12,18,46,50,14,17,13,79,22,42,92,14,11,55,8,42,7,16,44,
23,49,69,39,43,53,130,20,59,22,236,15,110,26,217,90,23,15,236,46,25,1
9,220,34,31,8,171,8,110,9,216,8,102,46,208,18,32,65,186,90,36,64,167,1
16,34,100,150,1,147,26,50,12,52,7,103,36,34,50,98,39,31,78,46,42,55,76
,85,44,52,21,152,1,193,88,26,1,133,68,45,74,30,30,101,117,51,37,41,9,1
56,21,94,49,27,27,90,10,56,58,16,2,160,180,4,53,55,183,2,93,48,120,15,
11,133,136,6,82,7,171,1

Original URL Where File was Located:

D:\local\Temp\tmp2CFD.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
Online Services:

FAX: (425) 708-0096 Microsoft Corporation

Attn: Online Services Custodian of Records

One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	08-17-2016 13:01:41 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	13711825, 13712405, 13281882, 13337689, 13281881, 13711685, 13711686, 13712041, 13337682, 13712042, 13712170, 13395344, 13712333, 13337686, 13281876, 13674862, 13711695

NCMEC Note #1

ECD-JPR 08-17-2016 12:55:44 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

NCMEC Note #2

ECD-JPR 08-17-2016 13:01:43 UTC

There are multiple reports on this target. Please see CT #13281882 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agencies listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 09-26-2016 17:02:38 UTC

Homeland Security Investigations

Investigator:

Title:	Caitlin Moynihan
City/State:	VT
Phone Number:	8026605016
Email Address:	caitlin.e.moynihan@ice.dhs.gov

Time/Date was made available: 09-26-2016 17:06:34 UTC

This concludes Section D

This concludes CyberTipline Report 13712450



CyberTipline Report 11614028

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 05-20-2016 17:09:22 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*

Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Section C: Additional Information Provided by NCMEC	4
NCMEC Note #1	4
NCMEC Note #2	4
Section D: Law Enforcement Contact Information	12
Vermont Office of Attorney General	12



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 01-01-0001 00:00:00 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
Peer to Peer Filenames: tmp8150.jpg

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename:	tmp8150.jpg
Was File Reviewed by Company?	Yes
Child Pornography Categorization by ESP: (See Section B for further explanation)	A1
Original Binary Hash of File (PhotoDNA):	10,51,0,92,35,31,3,85,23,91,10,171,71,15,5,119,13,42,0,49,17,20,8,34,36,249,13,159,93,37,0,249,48,64,20,163,113,16,24,98,33,76,1,140,72,12,4,109,5,255,96,11,26,40,28,46,29,8,8,86,146,34,13,140,60,157,44,113,179,14,18,54,1,198,146,15,3,181,88,23,8,25,31,38,80,7,24,75,101,90,58,74,134,20,59,23,0,225,7,66,4,190,17,62,19,42,44,17,60,30,43,27,172,2,65,18,60,8,150,3,0,255,18,62,10,80,39,43,39,26,62,45,38,41,64,25,209,1,41,8,94,5,53,3
Original URL Where File was Located:	D:\local\Temp\tmp8150.jpg

**Additional Information:****Where to serve legal process in Criminal Matters**

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other Online Services:

FAX: (425) 708-0096 Microsoft Corporation
Attn: Online Services Custodian of Records
One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 15:47:00 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-RHS 06-27-2016 19:40:55 UTC

Microsoft provided the following reported user information:

Screen Name: vt151231,78837c86b9c60032

IP Address: 24.91.154.58

NCMEC Note #2

ECD-NB 06-28-2016 16:02:53 UTC

I reviewed the uploaded file and found what appears to be apparent child pornography

=====

CT/TA search results for:

vt151231

78837c86b9c60032

24.91.154.58

11614028

11751258

11751259

12045016

12050728

12050735

12050739



12051516
12051925
12415510
12415511
12415578
12415755
12468560
12468566
12469951
12469960
12469962
12469964
12526149
12526150
12526151
12526152
12526153
12526155
12526156
12526157
12526159
12527752
12527760
12627552
12627584
12627589
12651690
12651697
12651701
12765571
12765579
12766078

=====

CT/TA Search results for : *jvt15123456* (from 12469951)

12468560
12468566
12469960
12469962
12469964

=====

CT/TA Search results for : *jvt1234515* (from 12527752)

12526149
12526150
12526151
12526152
12526153
12526155
12526156
12526157



12526159
12527752
12527760

=====

CT/TA Search results for : *jvt12345615* (from 12627589)

12627552
12627584
12627589
12651690
12651697
12651701

=====

CT/TA Search results for : *vtj12315* (from 12765571)

12765579
12766078

=====

CT/TA Search results for : *vt151233* (from 12050728)

12045016
12050735
12050739
12051516
12051925

=====

A WHOIS search for '24.91.154.58' yielded the following:

Address lookup

canonical name

c-24-91-154-58 . hsd1 . vt . comcast.net .

aliases

addresses

24.91.154.58

Network Whois record

Queried whois.arin.net with "n ! NET-24-91-128-0-1 "...

NetRange: 24.91.128.0 - 24.91.255.255

CIDR: 24.91.128.0/17

NetName: NEW-ENGLAND-7

NetHandle: NET-24-91-128-0-1

Parent: RW2-NORTHEAST-2 (NET-24-91-0-0-1)

NetType: Reassigned

OriginAS:

Customer: Comcast Cable Communications Holdings, Inc (C02610697)



RegDate: 2010-10-18
 Updated: 2010-10-18
 Ref: <https://whois.arin.net/rest/net/NET-24-91-128-0-1>
 CustName: Comcast Cable Communications Holdings, Inc
 Address: 1800 Bishops Gate Blvd
 City: Mt Laurel
 StateProv: NJ
 PostalCode: 08054
 Country: US
 RegDate: 2010-10-18
 Updated: 2011-03-19
 Ref: <https://whois.arin.net/rest/customer/C02610697>
 OrgAbuseHandle: NAPO-ARIN
 OrgAbuseName: Network Abuse and Policy Observance
 OrgAbusePhone: +1-888-565-4329
 OrgAbuseEmail: abuse@comcast.net
 OrgAbuseRef: <https://whois.arin.net/rest/poc/NAPO-ARIN>
 OrgTechHandle: IC161-ARIN
 OrgTechName: Comcast Cable Communications Inc
 OrgTechPhone: +1-856-317-7200
 OrgTechEmail: CNIPEO-lp-registration@cable.comcast.com
 OrgTechRef: <https://whois.arin.net/rest/poc/IC161-ARIN>

DNS records

```

name class type data time to live
c-24-91-154-58.hsd1.vt.comcast.net IN A 24.91.154.58 7200s (02:00:00)
hsd1.vt.comcast.net IN NS dns101.comcast.net 7200s (02:00:00)
hsd1.vt.comcast.net IN NS dns104.comcast.net 7200s (02:00:00)
hsd1.vt.comcast.net IN NS dns105.comcast.net 7200s (02:00:00)
hsd1.vt.comcast.net IN NS dns103.comcast.net 7200s (02:00:00)
hsd1.vt.comcast.net IN NS dns102.comcast.net 7200s (02:00:00)
hsd1.vt.comcast.net IN SOA server: dns101.comcast.net email: dnsadmin@comcast.net serial: 1351826 refresh: 7200
retry: 3600 expire: 604800 minimum ttl: 7200 7200s (02:00:00)
comcast.net IN A 69.252.80.75 30s (00:00:30)
comcast.net IN RRSIG type covered: A (1) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 30 (00:00:30) signature
expiration: 2016-07-05 00:23:38Z signature inception: 2016-06-27 21:18:38Z key tag: 44553 signer's name: comcast.net
signature:
(1024 bits) 3180B34AED6EB2388ED9968C137C3303
5B1A7EA6A9C5AA2030EEC2026A903B26
EF9E6572AA84FBD3422F1852D99F5556
CBB2ED560E976D2D6F9C3B9EC3013039
FDDEA2F9BCFC7F4D53E09DFF26185309
F335896F504F7D7EFE0ADE21082F6688
13F4CE1BF62ACF0CD48911CF82DF79DA
5A0C210B47097F37FC0835D15369AF26 30s (00:00:30)
comcast.net IN MX preference: 5 exchange: mx1.comcast.net 7200s (02:00:00)
comcast.net IN MX preference: 5 exchange: mx2.comcast.net 7200s (02:00:00)
comcast.net IN RRSIG type covered: MX (15) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 7200 (02:00:00) signature
expiration: 2016-07-05 00:23:38Z signature inception: 2016-06-27 21:18:38Z key tag: 44553 signer's name: comcast.net
signature:
(1024 bits) 7C2349A4639DFEE9FFEF53C9A2E3919A
10735E461745E339E941144A024AF229
  
```



79178CAC406365DEBFD80DF2C37B6D6F
F0221135412CE3DABF25290DF4DCDCAD
46A3E6ADD23DB4DFE66E4ADE198D7E8F
E6956BE91A1DD85AAECAC5BB0724D24C
F80B27A3A6AFA35366DF2A80CEFFFEFEB
2A608A767D5E3DB29B37B888943346D2 7200s (02:00:00)
comcast.net IN NS dns102.comcast.net 7200s (02:00:00)
comcast.net IN NS dns101.comcast.net 7200s (02:00:00)
comcast.net IN NS dns103.comcast.net 7200s (02:00:00)
comcast.net IN NS dns104.comcast.net 7200s (02:00:00)
comcast.net IN NS dns105.comcast.net 7200s (02:00:00)
comcast.net IN RRSIG type covered: NS (2) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 7200 (02:00:00) signature
expiration: 2016-07-05 00:23:38Z signature inception: 2016-06-27 21:18:38Z key tag: 44553 signer's name: comcast.net
signature:
(1024 bits) 9EC0F31E2F18BDE9801116AF00D4058F
F5F260039789F8BC5BE493D3A07345EC
2396979172E55B88145CC0AA33DC5C9C
9CAFFD529F37DF2351911382100E6CCA
B426293CDDDB059C9F5DD185CDAD322A2
15D9D03696EB9CA6E792F82DD6B5D9EF
8058AF290EFE6672265F15850F1CF6B4
D53BD9C5DD93574BA8860E8AF55E84A7 7200s (02:00:00)
comcast.net IN TXT v=spf1 ip4:96.114.154.128/25 ip4:69.252.207.0/25 include:_spf6.comcast.net include:_spf.mdp.comcast.net ?all
7200s (02:00:00)
comcast.net IN RRSIG type covered: TXT (16) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 7200 (02:00:00) signature
expiration: 2016-07-05 00:23:38Z signature inception: 2016-06-27 21:18:38Z key tag: 44553 signer's name: comcast.net
signature:
(1024 bits) 593ABBAE80F2D4FD7DDBB9BD187A9EE5
420F3730E78F4D5DEA1E570B45B1283C
686EEB1B34573158D7FE99B8785363F2
DEA713770691935C0136740939922958
C2BD1BE02E71157E2F4CCDA9F7E80E3D
8040EB0F7E7F6DE39B417006333D05BB
CECC933DE6E3E9D3357A5EDEF60BC79E
4EB82F1815CE0DB563BE5C13D53A323C 7200s (02:00:00)
comcast.net IN NSEC next domain name: 4gmobile.comcast.net record types: A NS SOA MX TXT RRSIG NSEC DNSKEY
3600s (01:00:00)
comcast.net IN RRSIG type covered: NSEC (47) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 3600 (01:00:00) signature
expiration: 2016-07-05 00:23:38Z signature inception: 2016-06-27 21:18:38Z key tag: 44553 signer's name: comcast.net
signature:
(1024 bits) 742926D80E679BED36738567B4DA8660
8F7C19336D9DB5FE37EB895977ABB1E7
AEA80F8DD81971E3097A551DF6E7D45E
557EAB282B599ADAE39FE88C79B21276
2E0467A3D2C7B97D1C5F335761AD762C
990AF63CEA81B9C302D4BE828FBB1B5C
603BDA025F4297A71AC1D4B40D3E052E
0AA02BBF950A2C83F43268A43E858E5D 3600s (01:00:00)
comcast.net IN DNSKEY flags: ZoneKey (256) protocol: 3 algorithm: RSA/SHA-1 (5) public key:
(1056 bits) 03010001CA97AA33D8252C366DFEFC49
7CF723676A27CC98507CC103DB63E7D3
6BC5386CB117903AA8C30556F0722F9C
C8878AEF6A0CB46EE2C4392A1EECB1F1



75DA4A5E1697D475A8302109DF494861
 1ED85D247B70F917CA36DBF0085118A7
 957D15F56555E71972CEA2C9DE89FE46
 071354117F189DECCE98DEBAE6697E95
 B72D858B 3600s (01:00:00)
 comcast.net IN DNSKEY flags: SecureEntryPoint, ZoneKey (257) protocol: 3 algorithm: RSA/SHA-1 (5) public key:
 (2080 bits) 03010001C753C17B8A204454A0468E1C
 211A7CF0A01D6F03ABC39FB433C3D6C6
 42C02507ED58DF49742982F918506FBA
 14DF4834FDAE1F26F345EFE6E041BC1C
 3F3390AB5A201CEB61921C6DC86E5CA6
 796E2C248F58483131A50C6D230F48F7
 AE3889924DDD0E4CA02AF57C16CC0426
 8F57EFE0966ED7F858A817AA777FD897
 2C9620CAE17BA316CC36EDE5A95E51D9
 B794AE41BD0DD6398C6B31125F060962
 D19771EE6F8B8A4186513D3948024259
 313F179DBDA7A54F984AC583F79481F8
 BE306B28CCD013B3B3A01E253AC25585
 BBC31755595330BA9F8DB0F165AF8C10
 D8DD38A53AFB02F497BB0CE0F7C90960
 726890F343CCE339277D027BE803F162
 BAE8C131 3600s (01:00:00)
 comcast.net IN RRSIG type covered: DNSKEY (48) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 3600 (01:00:00)
 signature expiration: 2016-10-18 21:23:38Z signature inception: 2016-06-20 17:23:38Z key tag: 40909 signer's name:
 comcast.net signature:
 (2048 bits) 336FDBCBA74E9D0D5950E01A3435157B
 8637A8500996E54C9F769EBE7F7739B3
 42B8D1595E054A80AD43D1F4D8A493EE
 F32DA95BD957ADD42C1C1E5DB7B463CA
 6E8184313CDE119686306398C384BD77
 724B665A659B709C691FC8588372031D
 D362D25FDF5336B193D510B6F1E9BA28
 A67569FB3BF0A7A32D36B84BE96FADE7
 B8B1FAA73D14085A46E42C5C29682687
 D32C5729F7A72BA01DDB01AC8DE96963
 28FB42E7ADB3C38C797465782629D299
 69997B123420DDF7DAE46CA0707AAE05
 B1274FBD835000F7A905989685AC5C0E
 87B15C7D0D09B4CA5CA0A94B9F5D3D23
 9271134B64803762B385B149034F856C
 A31C7E8699ED8236AA774C23094E5A38 3600s (01:00:00)
 comcast.net IN RRSIG type covered: DNSKEY (48) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 3600 (01:00:00)
 signature expiration: 2016-07-05 00:23:38Z signature inception: 2016-06-27 21:18:38Z key tag: 44553 signer's name:
 comcast.net signature:
 (1024 bits) 1A1656F5423BCA3ECE007B2A05241D47
 4BC37E9FCE7F833AC69D2345A30887CF
 09D75CB0871A16761BE3C156AEF057B2
 72DCC1089FEBD838EEAAECE069944FCA
 1FA7C9740F778BCF749E4414E86A4B70
 3E90FA771E423958E0E7B273FCAB017C
 FB8BF0F79708247BFB5902FA2F63BE5F
 A3FA8C71045A57826797025B950A9E87 3600s (01:00:00)



comcast.net IN SOA server: dns101.comcast.net email: domregtech@comcastonline.com serial: 2008188833 refresh: 7200
 retry: 3600 expire: 1209600 minimum ttl: 3600 7200s (02:00:00)
 comcast.net IN RRSIG type covered: SOA (6) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 7200 (02:00:00) signature
 expiration: 2016-07-05 00:23:38Z signature inception: 2016-06-27 21:18:38Z key tag: 44553 signer's name: comcast.net
 signature:
 (1024 bits) 7852689A3093F4BF3D6C0F567BAE5D2A
 79799A6A135BBD20292D7B3857C6EB55
 C53D23C38A8748B734EE014A00B137AB
 370402CD8627626E86C3EA76927E93BD
 C7E6EA0844B187C75B798DF31BAB79FE
 AD42217C777A4FE2D9A73BE79E5FC5FC
 594CE4A70795687FD410F2049E5D5536
 DDEFCFEAE06D7F1F8443E6367CB17875 7200s (02:00:00)
 58.154.91.24.in-addr.arpa IN PTR c-24-91-154-58.hsd1.vt.comcast.net 7200s (02:00:00)
 154.91.24.in-addr.arpa IN NS dns102.comcast.net 7200s (02:00:00)
 154.91.24.in-addr.arpa IN NS dns103.comcast.net 7200s (02:00:00)
 154.91.24.in-addr.arpa IN NS dns104.comcast.net 7200s (02:00:00)
 154.91.24.in-addr.arpa IN NS dns105.comcast.net 7200s (02:00:00)
 154.91.24.in-addr.arpa IN NS dns101.comcast.net 7200s (02:00:00)
 154.91.24.in-addr.arpa IN SOA server: dns101.comcast.net email: dnsadmin@comcast.net serial: 2139 refresh: 7200
 retry: 3600 expire: 604800 minimum ttl: 7200 7200s (02:00:00)

Traceroute

Tracing route to c-24-91-154-58.hsd1.vt.comcast.net [24.91.154.58] ... hop rtt rtt rtt ip address fully qualified
 domain name
 1 1 0 0 208.101.16.73 49.10.65d0.ip4.static.sl-reverse.com
 2 0 0 0 66.228.118.153 ae11.dar01.sr01.dal01.networklayer.com
 3 0 0 0 173.192.18.210 ae6.bbr01.eq01.dal03.networklayer.com
 4 0 0 0 75.149.228.33 be-111-pe03.1950stemmons.tx.ibone.comcast.net
 5 3 2 2 68.86.89.249 hu-0-4-0-9-cr02.dallas.tx.ibone.comcast.net
 6 16 17 16 68.86.84.229 be-11724-cr02.denver.co.ibone.comcast.net
 7 29 29 29 68.86.85.169 be-10517-cr02.350ecermak.il.ibone.comcast.net
 8 58 58 58 68.86.91.6 be-7922-ar01.woburn.ma.boston.comcast.net
 9 62 62 62 162.151.113.14
 10 61 64 61 68.85.142.62 te-1-0-0-ten02.bennington.vt.boston.comcast.net
 11 * * *
 12 * * *
 13 * * *
 14 * * *

Trace aborted

=====

Country: US
 Region: VT
 City: Bennington
 Postal Code: 05201
 Latitude: 42.8626
 Longitude: -73.0998
 Metropolitan Code: Albany-Schenectady-Troy
 ISP: Comcast Cable
 Organization: Comcast Cable



=====

Country: US
Region: VT
City: Bennington
Postal Code: 05201
Latitude: 42.8781345
Longitude: -73.1967741
Area: 12.507 sq. km. (4.829 sq. miles)

=====

VPN: Vermont Office of Attorney General Criminal Division

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:53 UTC

This concludes Section D

This concludes CyberTipline Report 11614028



CyberTipline Report 11751258

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 05-23-2016 19:15:43 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Section C: Additional Information Provided by NCMEC	4
NCMEC Note #1	4
NCMEC Note #2	4
NCMEC Note #3	4
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 01-01-0001 00:00:00 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
Peer to Peer Filenames: tmp36DA.jpg

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename:	tmp36DA.jpg
Was File Reviewed by Company?	Yes
Child Pornography Categorization by ESP: (See Section B for further explanation)	A2
Original Binary Hash of File (PhotoDNA):	52,88,65,17,44,87,105,36,125,8,52,22,84,43,62,22,66,93,56,109,16,134,7 0,38,87,78,27,87,50,90,86,126,99,23,22,82,120,10,31,40,62,91,110,37,24 ,110,59,39,21,24,11,95,30,22,2,118,110,6,12,79,234,6,56,52,51,136,64,5 6,37,56,60,28,10,60,72,15,27,12,122,26,167,23,134,28,239,50,122,57,24, 120,14,85,28,31,14,52,50,25,13,62,85,10,64,112,234,64,190,137,100,96, 57,130,52,184,3,125,105,24,17,72,38,12,0,88,63,13,3,121,140,11,11,232, 46,58,1,205,29,114,17,150,97,10,11,125
Original URL Where File was Located:	D:\local\Temp\tmp36DA.jpg

**Additional Information:****Where to serve legal process in Criminal Matters**

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other Online Services:

FAX: (425) 708-0096 Microsoft Corporation
Attn: Online Services Custodian of Records
One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A2: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-RHS 06-27-2016 19:42:47 UTC

Microsoft provided the following reported user information:

Screen Name: vt151232
IP Address: 24.91.154.58

NCMEC Note #2

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #3

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.



For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 11751258



CyberTipline Report 11751259

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 05-23-2016 19:15:43 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*

Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Section C: Additional Information Provided by NCMEC	4
NCMEC Note #1	4
NCMEC Note #2	4
NCMEC Note #3	4
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 01-01-0001 00:00:00 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
Peer to Peer Filenames: tmp36EB.jpg

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp36EB.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A1
(See Section B for further explanation)
Original Binary Hash of File (PhotoDNA): 1,114,24,7,39,11,57,1,187,0,82,1,242,3,147,20,25,5,38,37,3,2,0,39,17,60,17,28,61,3,53,8,255,20,143,25,160,81,51,189,73,28,0,138,39,34,15,95,46,21,21,9,114,0,62,17,178,73,93,138,58,150,8,186,157,22,0,222,149,19,16,150,40,56,29,20,144,3,41,31,43,65,63,41,13,84,102,33,60,17,58,62,183,6,45,101,14,126,115,1,164,10,63,6,114,22,116,25,37,122,214,76,15,84,100,76,50,11,44,99,6,90,75,12,125,16,77,1,71,50,57,60,17,152,15,127,0,85,11,100,13,7,0,80
Original URL Where File was Located: D:\local\Temp\tmp36EB.jpg

**Additional Information:****Where to serve legal process in Criminal Matters**

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other Online Services:

FAX: (425) 708-0096 Microsoft Corporation
Attn: Online Services Custodian of Records
One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-RHS 06-27-2016 19:42:31 UTC

Microsoft provided the following reported user information:

Screen Name: vt151232
IP Address: 24.91.154.58

NCMEC Note #2

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #3

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.



For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 11751259



CyberTipline Report 11855790

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 05-26-2016 17:59:42 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Section C: Additional Information Provided by NCMEC	4
NCMEC Note #1	4
NCMEC Note #2	4
Section D: Law Enforcement Contact Information	10
Vermont Office of Attorney General	10



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 01-01-0001 00:00:00 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
Peer to Peer Filenames: tmpACCC.jpg

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename:	tmpACCC.jpg
Was File Reviewed by Company?	Yes
Child Pornography Categorization by ESP: (See Section B for further explanation)	A1
Original Binary Hash of File (PhotoDNA):	10,51,0,92,35,31,3,85,23,91,10,171,71,15,5,119,13,42,0,49,17,20,8,34,36,249,13,159,93,37,0,249,48,64,20,163,113,16,24,98,33,76,1,140,72,12,4,109,5,255,96,11,26,40,28,46,29,8,8,86,146,34,13,140,60,157,44,113,179,14,18,54,1,198,146,15,3,181,88,23,8,25,31,38,80,7,24,75,101,90,58,74,134,20,59,23,0,225,7,66,4,190,17,62,19,42,44,17,60,30,43,27,172,2,65,18,60,8,150,3,0,255,18,62,10,80,39,43,39,26,62,45,38,41,64,25,209,1,41,8,94,5,53,3
Original URL Where File was Located:	D:\local\Temp\tmpACCC.jpg

**Additional Information:****Where to serve legal process in Criminal Matters**

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other Online Services:

FAX: (425) 708-0096 Microsoft Corporation
Attn: Online Services Custodian of Records
One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level: E (Report submitted by a registered Electronic Service Provider)
 NCMEC Classification: Apparent Child Pornography
 NCMEC Date Processed: 06-30-2016 15:11:07 UTC
 Made Available to Law Enforcement by NCMEC: Yes

NCMEC Note #1

ECD-RHS 06-29-2016 18:43:07 UTC

Microsoft provided the following reported user information:

Screen Name: v15t1231,be6df84858f5b381
 IP Address: 24.91.154.58

NCMEC Note #2

ECD-NB 06-30-2016 15:11:07 UTC

I reviewed the uploaded file and found what appears to be apparent child pornography

=====

Negative CT/TA results for:

v15t1231
 be6df84858f5b381
 24.91.154.58

=====

A WHOIS search for '24.91.154.58' yielded:

Address lookup

canonical name
 c-24-91-154-58 . hsd1 . vt . comcast.net .

aliases



addresses

24.91.154.58

Network Whois record

Queried whois.arin.net with "n ! NET-24-91-128-0-1 "...
 NetRange: 24.91.128.0 - 24.91.255.255
 CIDR: 24.91.128.0/17
 NetName: NEW-ENGLAND-7
 NetHandle: NET-24-91-128-0-1
 Parent: RW2-NORTHEAST-2 (NET-24-91-0-0-1)
 NetType: Reassigned
 OriginAS:
 Customer: Comcast Cable Communications Holdings, Inc (C02610697)
 RegDate: 2010-10-18
 Updated: 2010-10-18
 Ref: <https://whois.arin.net/rest/net/NET-24-91-128-0-1>
 CustName: Comcast Cable Communications Holdings, Inc
 Address: 1800 Bishops Gate Blvd
 City: Mt Laurel
 StateProv: NJ
 PostalCode: 08054
 Country: US
 RegDate: 2010-10-18
 Updated: 2011-03-19
 Ref: <https://whois.arin.net/rest/customer/C02610697>
 OrgAbuseHandle: NAPO-ARIN
 OrgAbuseName: Network Abuse and Policy Observance
 OrgAbusePhone: +1-888-565-4329
 OrgAbuseEmail: abuse@comcast.net
 OrgAbuseRef: <https://whois.arin.net/rest/poc/NAPO-ARIN>
 OrgTechHandle: IC161-ARIN
 OrgTechName: Comcast Cable Communications Inc
 OrgTechPhone: +1-856-317-7200
 OrgTechEmail: CNIPEO-lp-registration@cable.comcast.com
 OrgTechRef: <https://whois.arin.net/rest/poc/IC161-ARIN>

DNS records

name	class	type	data	time to live
c-24-91-154-58.hsd1.vt.comcast.net	IN	A	24.91.154.58	7200s (02:00:00)
hsd1.vt.comcast.net	IN	NS	dns103.comcast.net	7200s (02:00:00)
hsd1.vt.comcast.net	IN	NS	dns102.comcast.net	7200s (02:00:00)
hsd1.vt.comcast.net	IN	NS	dns101.comcast.net	7200s (02:00:00)
hsd1.vt.comcast.net	IN	NS	dns104.comcast.net	7200s (02:00:00)
hsd1.vt.comcast.net	IN	NS	dns105.comcast.net	7200s (02:00:00)
hsd1.vt.comcast.net	IN	SOA	server: dns101.comcast.net email: dnsadmin@comcast.net serial: 1351826 refresh: 7200 retry: 3600 expire: 604800 minimum ttl: 7200	7200s (02:00:00)
comcast.net	IN	A	69.252.80.75	30s (00:00:30)
comcast.net	IN	RRSIG	type covered: A (1) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 30 (00:00:30) signature expiration: 2016-07-05 00:23:38Z signature inception: 2016-06-27 21:18:38Z key tag: 44553 signer's name: comcast.net	



signature:

(1024 bits) 3180B34AED6EB2388ED9968C137C3303

5B1A7EA6A9C5AA2030EEC2026A903B26

EF9E6572AA84FBD3422F1852D99F5556

CBB2ED560E976D2D6F9C3B9EC3013039

FDDEA2F9BCFC7F4D53E09DFF26185309

F335896F504F7D7EFE0ADE21082F6688

13F4CE1BF62ACF0CD48911CF82DF79DA

5A0C210B47097F37FC0835D15369AF26 30s (00:00:30)

comcast.net IN MX preference: 5 exchange: mx2.comcast.net 7200s (02:00:00)

comcast.net IN MX preference: 5 exchange: mx1.comcast.net 7200s (02:00:00)

comcast.net IN RRSIG type covered: MX (15) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 7200 (02:00:00) signature

expiration: 2016-07-05 00:23:38Z signature inception: 2016-06-27 21:18:38Z key tag: 44553 signer's name: comcast.net

signature:

(1024 bits) 7C2349A4639DFEE9FFEF53C9A2E3919A

10735E461745E339E941144A024AF229

79178CAC406365DEBFD80DF2C37B6D6F

F0221135412CE3DABF25290DF4DCDCAD

46A3E6ADD23DB4DFE66E4ADE198D7E8F

E6956BE91A1DD85AAECAC5BB0724D24C

F80B27A3A6AFA35366DF2A80CEFFEFEB

2A608A767D5E3DB29B37B888943346D2 7200s (02:00:00)

comcast.net IN NS dns104.comcast.net 7200s (02:00:00)

comcast.net IN NS dns105.comcast.net 7200s (02:00:00)

comcast.net IN NS dns102.comcast.net 7200s (02:00:00)

comcast.net IN NS dns101.comcast.net 7200s (02:00:00)

comcast.net IN NS dns103.comcast.net 7200s (02:00:00)

comcast.net IN RRSIG type covered: NS (2) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 7200 (02:00:00) signature

expiration: 2016-07-05 00:23:38Z signature inception: 2016-06-27 21:18:38Z key tag: 44553 signer's name: comcast.net

signature:

(1024 bits) 9EC0F31E2F18BDE9801116AF00D4058F

F5F260039789F8BC5BE493D3A07345EC

2396979172E55B88145CC0AA33DC5C9C

9CAFFD529F37DF2351911382100E6CCA

B426293CDDDB059C9F5DD185CDAD322A2

15D9D03696EB9CA6E792F82DD6B5D9EF

8058AF290EFE6672265F15850F1CF6B4

D53BD9C5DD93574BA8860E8AF55E84A7 7200s (02:00:00)

comcast.net IN TXT v=spf1 ip4:96.114.154.128/25 ip4:69.252.207.0/25 include:_spf6.comcast.net include:_spf.mdp.comcast.net ?all 7200s (02:00:00)

comcast.net IN RRSIG type covered: TXT (16) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 7200 (02:00:00) signature

expiration: 2016-07-05 00:23:38Z signature inception: 2016-06-27 21:18:38Z key tag: 44553 signer's name: comcast.net

signature:

(1024 bits) 593ABBAE80F2D4FD7DDBB9BD187A9EE5

420F3730E78F4D5DEA1E570B45B1283C

686EEB1B34573158D7FE99B8785363F2

DEA713770691935C0136740939922958

C2BD1BE02E71157E2F4CCDA9F7E80E3D

8040EB0F7E7F6DE39B417006333D05BB

CECC933DE6E3E9D3357A5EDEF60BC79E

4EB82F1815CE0DB563BE5C13D53A323C 7200s (02:00:00)

comcast.net IN NSEC next domain name: 4gmobile.comcast.net record types: A NS SOA MX TXT RRSIG NSEC DNSKEY

3600s (01:00:00)



comcast.net IN RRSIG type covered: NSEC (47) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 3600 (01:00:00) signature expiration: 2016-07-05 00:23:38Z signature inception: 2016-06-27 21:18:38Z key tag: 44553 signer's name: comcast.net signature:

(1024 bits) 742926D80E679BED36738567B4DA8660

8F7C19336D9DB5FE37EB895977ABB1E7

AEA80F8DD81971E3097A551DF6E7D45E

557EAB282B599ADAE39FE88C79B21276

2E0467A3D2C7B97D1C5F335761AD762C

990AF63CEA81B9C302D4BE828FBB1B5C

603BDA025F4297A71AC1D4B40D3E052E

0AA02BBF950A2C83F43268A43E858E5D 3600s (01:00:00)

comcast.net IN DNSKEY flags: ZoneKey (256) protocol: 3 algorithm: RSA/SHA-1 (5) public key:

(1056 bits) 03010001CA97AA33D8252C366DFEFC49

7CF723676A27CC98507CC103DB63E7D3

6BC5386CB117903AA8C30556F0722F9C

C8878AEF6A0CB46EE2C4392A1EECB1F1

75DA4A5E1697D475A8302109DF494861

1ED85D247B70F917CA36DBF0085118A7

957D15F56555E71972CEA2C9DE89FE46

071354117F189DECCE98DEBAE6697E95

B72D858B 3600s (01:00:00)

comcast.net IN DNSKEY flags: SecureEntryPoint, ZoneKey (257) protocol: 3 algorithm: RSA/SHA-1 (5) public key:

(2080 bits) 03010001C753C17B8A204454A0468E1C

211A7CF0A01D6F03ABC39FB433C3D6C6

42C02507ED58DF49742982F918506FBA

14DF4834FDAE1F26F345EFE6E041BC1C

3F3390AB5A201CEB61921C6DC86E5CA6

796E2C248F58483131A50C6D230F48F7

AE3889924DDD0E4CA02AF57C16CC0426

8F57EFE0966ED7F858A817AA777FD897

2C9620CAE17BA316CC36EDE5A95E51D9

B794AE41BD0DD6398C6B31125F060962

D19771EE6F8B8A4186513D3948024259

313F179DBDA7A54F984AC583F79481F8

BE306B28CCD013B3B3A01E253AC25585

BBC31755595330BA9F8DB0F165AF8C10

D8DD38A53AFB02F497BB0CE0F7C90960

726890F343CCE339277D027BE803F162

BAE8C131 3600s (01:00:00)

comcast.net IN RRSIG type covered: DNSKEY (48) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 3600 (01:00:00)

signature expiration: 2016-07-05 00:23:38Z signature inception: 2016-06-27 21:18:38Z key tag: 44553 signer's name:

comcast.net signature:

(1024 bits) 1A1656F5423BCA3ECE007B2A05241D47

4BC37E9FCE7F833AC69D2345A30887CF

09D75CB0871A16761BE3C156AEF057B2

72DCC1089FEBD838EEAAECE069944FCA

1FA7C9740F778BCF749E4414E86A4B70

3E90FA771E423958E0E7B273FCAB017C

FB8BF0F79708247BFB5902FA2F63BE5F

A3FA8C71045A57826797025B950A9E87 3600s (01:00:00)

comcast.net IN RRSIG type covered: DNSKEY (48) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 3600 (01:00:00)

signature expiration: 2016-10-18 21:23:38Z signature inception: 2016-06-20 17:23:38Z key tag: 40909 signer's name:

comcast.net signature:



(2048 bits) 336FDBCBA74E9D0D5950E01A3435157B
 8637A8500996E54C9F769EBE7F7739B3
 42B8D1595E054A80AD43D1F4D8A493EE
 F32DA95BD957ADD42C1C1E5DB7B463CA
 6E8184313CDE119686306398C384BD77
 724B665A659B709C691FC8588372031D
 D362D25FDF5336B193D510B6F1E9BA28
 A67569FB3BF0A7A32D36B84BE96FADE7
 B8B1FAA73D14085A46E42C5C29682687
 D32C5729F7A72BA01DDB01AC8DE96963
 28FB42E7ADB3C38C797465782629D299
 69997B123420DDF7DAE46CA0707AAE05
 B1274FBD835000F7A905989685AC5C0E
 87B15C7D0D09B4CA5CA0A94B9F5D3D23
 9271134B64803762B385B149034F856C
 A31C7E8699ED8236AA774C23094E5A38 3600s (01:00:00)
 comcast.net IN SOA server: dns101.comcast.net email: domregtech@comcastonline.com serial: 2008188886 refresh: 7200
 retry: 3600 expire: 1209600 minimum ttl: 3600 7200s (02:00:00)
 comcast.net IN RRSIG type covered: SOA (6) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 7200 (02:00:00) signature
 expiration: 2016-07-05 00:23:38Z signature inception: 2016-06-27 21:18:38Z key tag: 44553 signer's name: comcast.net
 signature:
 (1024 bits) 292DFBD96DCA44E7EDE9C9789636B6AC
 406C142DE8BC62C1EB40BF5FF7A0DA29
 C6438EDD6107B6CB1738023489DF4A3A
 4265E46EC82B5AB68AF9B942ADB0B400
 0ADB82BE508FBAD59933692DB9E7DA1C
 AD35CD2AE91DFCE85173EEDA77526BAA
 A02F77BF4022D680839A9FFF88EF4AFD
 967648E00B5FE18D62BCDC196DBB44D1 7200s (02:00:00)
 58.154.91.24.in-addr.arpa IN PTR c-24-91-154-58.hsd1.vt.comcast.net 7200s (02:00:00)
 154.91.24.in-addr.arpa IN NS dns105.comcast.net 7200s (02:00:00)
 154.91.24.in-addr.arpa IN NS dns101.comcast.net 7200s (02:00:00)
 154.91.24.in-addr.arpa IN NS dns102.comcast.net 7200s (02:00:00)
 154.91.24.in-addr.arpa IN NS dns103.comcast.net 7200s (02:00:00)
 154.91.24.in-addr.arpa IN NS dns104.comcast.net 7200s (02:00:00)
 154.91.24.in-addr.arpa IN SOA server: dns101.comcast.net email: dnsadmin@comcast.net serial: 2139 refresh: 7200
 retry: 3600 expire: 604800 minimum ttl: 7200 7200s (02:00:00)

Traceroute

Tracing route to c-24-91-154-58.hsd1.vt.comcast.net [24.91.154.58] ...

hop	rtt	rtt	rtt	ip address	fully qualified
1	1	0	0	208.101.16.73	49.10.65d0.ip4.static.sl-reverse.com
2	0	0	0	66.228.118.153	ae11.dar01.sr01.dal01.networklayer.com
3	0	0	0	173.192.18.210	ae6.bbr01.eq01.dal03.networklayer.com
4	0	0	0	75.149.228.33	be-111-pe03.1950stemmons.tx.ibone.comcast.net
5	1	2	2	68.86.86.169	hu-0-4-0-0-cr02.dallas.tx.ibone.comcast.net
6	16	16	16	68.86.84.229	be-11724-cr02.denver.co.ibone.comcast.net
7	30	29	29	68.86.85.169	be-10517-cr02.350ecermak.il.ibone.comcast.net
8	57	57	58	68.86.91.6	be-7922-ar01.woburn.ma.boston.comcast.net
9	62	62	62	162.151.113.14	
10	64	62	65	68.85.143.46	te-3-0-0-ten02.bennington.vt.boston.comcast.net
11	*	*	*		



12 * * *
 13 * * *
 14 * * *

Trace aborted

==

Country: US
 Region: VT
 City: Bennington
 Postal Code: 05201
 Latitude: 42.8626
 Longitude: -73.0998
 Metropolitan Code: Albany-Schenectady-Troy
 ISP: Comcast Cable
 Organization: Comcast Cable

==

Country: US
 Region: VT
 City: Bennington
 Postal Code: 05201
 Latitude: 42.8781345
 Longitude: -73.1967741
 Area: 12.507 sq. km. (4.829 sq. miles)

=====

VPN: Vermont Office of Attorney General

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-30-2016 15:11:07 UTC

This concludes Section D

This concludes CyberTipline Report 11855790



CyberTipline Report 12045016

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 05-31-2016 15:38:30 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Section C: Additional Information Provided by NCMEC	4
NCMEC Note #1	4
NCMEC Note #2	4
NCMEC Note #3	4
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 01-01-0001 00:00:00 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
Peer to Peer Filenames: tmp2110.jpg

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename:	tmp2110.jpg
Was File Reviewed by Company?	Yes
Child Pornography Categorization by ESP: (See Section B for further explanation)	A1
Original Binary Hash of File (PhotoDNA):	112,1,99,12,49,20,41,41,4,76,3,97,43,38,18,61,21,79,49,16,19,50,24,17,6 9,42,24,67,32,103,10,175,20,156,6,255,150,13,4,215,125,89,33,61,32,11 1,25,32,91,39,18,145,39,203,41,111,39,106,92,103,198,23,126,75,140,94 19,124,38,46,12,31,95,55,85,23,64,184,109,28,121,79,194,39,96,75,113, 37,64,33,42,33,102,1,97,1,50,119,117,19,50,176,40,97,160,63,46,111,84, 106,70,33,106,23,69,4,115,2,69,1,2,99,85,6,3,191,89,14,107,18,82,22,91, 35,100,11,110,34,68,0,60,25,32,8
Original URL Where File was Located:	D:\local\Temp\tmp2110.jpg

**Additional Information:****Where to serve legal process in Criminal Matters**

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other Online Services:

FAX: (425) 708-0096 Microsoft Corporation
Attn: Online Services Custodian of Records
One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-RHS 06-27-2016 19:41:50 UTC

Microsoft provided the following reported user information:

Screen Name: vt151233
IP Address: 24.91.154.58

NCMEC Note #2

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #3

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.



For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12045016



CyberTipline Report 12050728

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 05-31-2016 19:08:01 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Section C: Additional Information Provided by NCMEC	4
NCMEC Note #1	4
NCMEC Note #2	4
NCMEC Note #3	4
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 01-01-0001 00:00:00 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
Peer to Peer Filenames: tmpF14A.jpg

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename:	tmpF14A.jpg
Was File Reviewed by Company?	Yes
Child Pornography Categorization by ESP: (See Section B for further explanation)	A1
Original Binary Hash of File (PhotoDNA):	51,5,7,25,167,6,8,36,41,25,48,19,51,64,59,20,47,56,46,26,40,2,15,23,55,16,21,31,194,15,26,39,51,33,10,121,37,99,11,179,33,81,21,255,110,6,20,168,65,2,40,11,149,29,40,44,39,106,61,77,22,180,45,142,107,51,60,78,199,0,73,29,50,4,21,45,167,26,42,63,54,216,86,81,54,107,72,84,146,50,78,27,166,2,83,6,53,18,2,86,181,6,6,123,136,153,116,52,24,168,126,27,236,24,116,24,93,6,62,11,11,44,12,13,143,2,1,79,182,32,14,96,14,160,84,34,140,22,57,50,85,0,6,42
Original URL Where File was Located:	D:\local\Temp\tmpF14A.jpg

**Additional Information:****Where to serve legal process in Criminal Matters**

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other Online Services:

FAX: (425) 708-0096 Microsoft Corporation
Attn: Online Services Custodian of Records
One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-RHS 06-27-2016 19:41:54 UTC

Microsoft provided the following reported user information:

Screen Name: vt151233
IP Address: 24.91.154.58

NCMEC Note #2

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #3

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.



For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12050728



CyberTipline Report 12050735

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 05-31-2016 19:08:03 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Section C: Additional Information Provided by NCMEC	4
NCMEC Note #1	4
NCMEC Note #2	4
NCMEC Note #3	4
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 01-01-0001 00:00:00 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
Peer to Peer Filenames: tmpFC0F.jpg

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename:	tmpFC0F.jpg
Was File Reviewed by Company?	Yes
Child Pornography Categorization by ESP: (See Section B for further explanation)	A1
Original Binary Hash of File (PhotoDNA):	71,111,9,74,7,124,68,25,38,35,66,44,120,10,20,80,113,17,4,168,20,53,2,150,140,75,43,39,76,177,134,60,34,117,59,89,77,56,26,132,39,84,11,250,68,21,6,243,186,28,18,157,41,240,44,190,55,128,36,126,48,54,62,81,29,68,47,52,56,24,50,38,127,25,76,108,47,173,50,120,67,78,64,108,82,49,50,144,85,82,112,68,106,26,114,41,38,56,92,113,15,154,75,95,32,83,91,87,80,15,99,70,83,19,43,71,70,31,27,87,31,10,0,116,31,45,20,73,26,76,54,47,51,20,36,59,28,24,6,61,6,38,4,79
Original URL Where File was Located:	D:\local\Temp\tmpFC0F.jpg

**Additional Information:****Where to serve legal process in Criminal Matters**

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other Online Services:

FAX: (425) 708-0096 Microsoft Corporation
Attn: Online Services Custodian of Records
One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-RHS 06-27-2016 19:41:56 UTC

Microsoft provided the following reported user information:

Screen Name: vt151233
IP Address: 24.91.154.58

NCMEC Note #2

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #3

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.



For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12050735



CyberTipline Report 12050739

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 05-31-2016 19:08:05 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Section C: Additional Information Provided by NCMEC	4
NCMEC Note #1	4
NCMEC Note #2	4
NCMEC Note #3	4
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 01-01-0001 00:00:00 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
Peer to Peer Filenames: tmp134.jpg

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename:	tmp134.jpg
Was File Reviewed by Company?	Yes
Child Pornography Categorization by ESP: (See Section B for further explanation)	A1
Original Binary Hash of File (PhotoDNA):	165,0,0,82,143,66,15,96,3,113,23,82,35,12,22,110,87,4,46,113,52,11,49,89,155,0,20,19,194,134,58,74,25,159,44,143,61,28,36,133,116,12,36,162,114,16,35,113,165,3,94,11,163,197,93,93,33,127,139,41,53,30,128,14,53,37,53,46,137,4,18,115,152,18,59,40,140,92,112,72,90,105,212,54,28,128,165,14,9,79,83,15,36,18,37,25,191,23,168,10,81,87,118,34,68,74,33,79,79,88,82,89,17,96,136,18,12,90,112,3,29,43,84,9,21,99,26,53,11,69,21,54,29,21,5,90,53,26,24,53,26,104,33,16
Original URL Where File was Located:	D:\local\Temp\tmp134.jpg

**Additional Information:****Where to serve legal process in Criminal Matters**

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other Online Services:

FAX: (425) 708-0096 Microsoft Corporation

Attn: Online Services Custodian of Records

One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-RHS 06-27-2016 19:41:58 UTC

Microsoft provided the following reported user information:

Screen Name: vt151233
IP Address: 24.91.154.58

NCMEC Note #2

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #3

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.



For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12050739



CyberTipline Report 12051516

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 05-31-2016 19:26:03 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*

Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Section C: Additional Information Provided by NCMEC	4
NCMEC Note #1	4
NCMEC Note #2	4
NCMEC Note #3	4
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 01-01-0001 00:00:00 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
Peer to Peer Filenames: tmp76FE.jpg

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename:	tmp76FE.jpg
Was File Reviewed by Company?	Yes
Child Pornography Categorization by ESP: (See Section B for further explanation)	A1
Original Binary Hash of File (PhotoDNA):	10,51,0,92,35,31,3,85,23,91,10,171,71,15,5,119,13,42,0,49,17,20,8,34,36,249,13,159,93,37,0,249,48,64,20,163,113,16,24,98,33,76,1,140,72,12,4,109,5,255,96,11,26,40,28,46,29,8,8,86,146,34,13,140,60,157,44,113,179,14,18,54,1,198,146,15,3,181,88,23,8,25,31,38,80,7,24,75,101,90,58,74,134,20,59,23,0,225,7,66,4,190,17,62,19,42,44,17,60,30,43,27,172,2,65,18,60,8,150,3,0,255,18,62,10,80,39,43,39,26,62,45,38,41,64,25,209,1,41,8,94,5,53,3
Original URL Where File was Located:	D:\local\Temp\tmp76FE.jpg

**Additional Information:****Where to serve legal process in Criminal Matters**

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other Online Services:

FAX: (425) 708-0096 Microsoft Corporation
Attn: Online Services Custodian of Records
One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-RHS 06-27-2016 19:41:38 UTC

Microsoft provided the following reported user information:

Screen Name: vt151233,1c05ea5c5c990477

IP Address: 24.91.154.58

NCMEC Note #2

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #3

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.



For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12051516



CyberTipline Report 12051925

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 05-31-2016 19:33:54 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Section C: Additional Information Provided by NCMEC	4
NCMEC Note #1	4
NCMEC Note #2	4
NCMEC Note #3	4
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 01-01-0001 00:00:00 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
Peer to Peer Filenames: tmpA4FE.jpg

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename:	tmpA4FE.jpg
Was File Reviewed by Company?	Yes
Child Pornography Categorization by ESP: (See Section B for further explanation)	A1
Original Binary Hash of File (PhotoDNA):	10,51,0,92,35,31,3,85,23,91,10,171,71,15,5,119,13,42,0,49,17,20,8,34,36,249,13,159,93,37,0,249,48,64,20,163,113,16,24,98,33,76,1,140,72,12,4,109,5,255,96,11,26,40,28,46,29,8,8,86,146,34,13,140,60,157,44,113,179,14,18,54,1,198,146,15,3,181,88,23,8,25,31,38,80,7,24,75,101,90,58,74,134,20,59,23,0,225,7,66,4,190,17,62,19,42,44,17,60,30,43,27,172,2,65,18,60,8,150,3,0,255,18,62,10,80,39,43,39,26,62,45,38,41,64,25,209,1,41,8,94,5,53,3
Original URL Where File was Located:	D:\local\Temp\tmpA4FE.jpg

**Additional Information:****Where to serve legal process in Criminal Matters**

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other Online Services:

FAX: (425) 708-0096 Microsoft Corporation
Attn: Online Services Custodian of Records
One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-RHS 06-27-2016 19:41:41 UTC

Microsoft provided the following reported user information:

Screen Name: vt151233,1c05ea5c5c990477

IP Address: 24.91.154.58

NCMEC Note #2

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #3

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.



For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12051925



CyberTipline Report 12114079

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-02-2016 16:22:17 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Section C: Additional Information Provided by NCMEC	4
NCMEC Note #1	4
NCMEC Note #2	4
Section D: Law Enforcement Contact Information	5
Vermont Office of Attorney General	5



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 01-01-0001 00:00:00 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
Peer to Peer Filenames: tmpAE0C.jpg

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename:	tmpAE0C.jpg
Was File Reviewed by Company?	Yes
Child Pornography Categorization by ESP: (See Section B for further explanation)	A1
Original Binary Hash of File (PhotoDNA):	52,88,65,17,44,87,105,36,125,8,52,22,84,43,62,22,66,93,56,109,16,134,7 0,38,87,78,27,87,50,90,86,126,99,23,22,82,120,10,31,40,62,91,110,37,24 ,110,59,39,21,24,11,95,30,22,2,118,110,6,12,79,234,6,56,52,51,136,64,5 6,37,56,60,28,10,60,72,15,27,12,122,26,167,23,134,28,239,50,122,57,24, 120,14,85,28,31,14,52,50,25,13,62,85,10,64,112,234,64,190,137,100,96, 57,130,52,184,3,125,105,24,17,72,38,12,0,88,63,13,3,121,140,11,11,232, 46,58,1,205,29,114,17,150,97,10,11,125
Original URL Where File was Located:	D:\local\Temp\tmpAE0C.jpg

**Additional Information:****Where to serve legal process in Criminal Matters**

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other Online Services:

FAX: (425) 708-0096 Microsoft Corporation
Attn: Online Services Custodian of Records
One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	07-12-2016 16:15:37 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12116763, 12114080, 12114081

NCMEC Note #1

ECD-LB 07-11-2016 20:43:36 UTC

Microsoft provided the following reported user information:

Screen Name: vt151234

IP Address: 24.91.154.58

Event Time Stamp: 6/1/2016 9:11:42 PM +00:00

NCMEC Note #2

ECD-KDS 07-12-2016 16:15:37 UTC

There are multiple reports on this target. Please see CT #12116763 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 07-12-2016 16:15:37 UTC

This concludes Section D

This concludes CyberTipline Report 12114079



CyberTipline Report 12114080

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-02-2016 16:22:18 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*

Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Section C: Additional Information Provided by NCMEC	4
NCMEC Note #1	4
NCMEC Note #2	4
Section D: Law Enforcement Contact Information	5
Vermont Office of Attorney General	5



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 01-01-0001 00:00:00 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
Peer to Peer Filenames: tmpAEE8.jpg

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename:	tmpAEE8.jpg
Was File Reviewed by Company?	Yes
Child Pornography Categorization by ESP: (See Section B for further explanation)	A1
Original Binary Hash of File (PhotoDNA):	1,102,196,25,12,52,120,16,28,14,100,2,135,6,197,26,77,51,255,32,28,40,224,24,2,198,47,105,10,55,39,68,54,25,25,60,151,87,40,154,123,45,19,198,47,96,33,170,45,157,29,51,23,145,36,70,70,48,35,106,99,93,29,97,123,25,27,89,133,14,89,37,69,83,39,31,20,150,41,22,113,34,108,22,47,132,97,21,220,13,72,33,158,7,102,53,71,44,21,36,22,135,45,18,78,31,16,53,78,65,62,74,141,49,122,67,45,70,47,157,33,17,4,28,16,86,29,28,28,39,19,21,50,5,6,34,110,25,25,94,32,135,44,94
Original URL Where File was Located:	D:\local\Temp\tmpAEE8.jpg

**Additional Information:****Where to serve legal process in Criminal Matters**

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other Online Services:

FAX: (425) 708-0096 Microsoft Corporation
Attn: Online Services Custodian of Records
One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	07-12-2016 16:15:37 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12116763, 12114079, 12114081

NCMEC Note #1

ECD-LB 07-11-2016 20:44:07 UTC

Microsoft provided the following reported user information:

Screen Name: vt151234

IP Address: 24.91.154.58

Event Time Stamp: 6/1/2016 9:12:08 PM +00:00

NCMEC Note #2

ECD-KDS 07-12-2016 16:15:37 UTC

There are multiple reports on this target. Please see CT #12116763 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 07-12-2016 16:15:37 UTC

This concludes Section D

This concludes CyberTipline Report 12114080



CyberTipline Report 12114081

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-02-2016 16:22:18 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*

Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Section C: Additional Information Provided by NCMEC	4
NCMEC Note #1	4
NCMEC Note #2	4
Section D: Law Enforcement Contact Information	5
Vermont Office of Attorney General	5



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 01-01-0001 00:00:00 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
Peer to Peer Filenames: tmpAFA4.jpg

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename:	tmpAFA4.jpg
Was File Reviewed by Company?	Yes
Child Pornography Categorization by ESP: (See Section B for further explanation)	A1
Original Binary Hash of File (PhotoDNA):	2,110,23,12,43,10,63,2,199,0,83,2,234,6,114,34,13,6,16,55,6,6,1,56,21,4 9,18,25,68,2,55,8,255,27,155,34,143,101,44,208,94,31,0,144,51,38,19,86 ,48,21,19,10,117,0,56,19,160,76,72,142,50,146,6,168,154,20,2,222,164,1 5,13,164,38,60,34,20,151,4,42,31,44,67,71,31,14,84,122,24,56,20,68,45, 177,6,52,85,13,132,117,1,164,10,66,5,118,20,111,26,41,127,199,82,15,9 2,93,83,45,12,40,106,6,87,71,12,125,16,75,1,70,54,56,62,16,154,14,123, 0,86,11,95,14,7,1,74
Original URL Where File was Located:	D:\local\Temp\tmpAFA4.jpg

**Additional Information:****Where to serve legal process in Criminal Matters**

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other Online Services:

FAX: (425) 708-0096 Microsoft Corporation
Attn: Online Services Custodian of Records
One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	07-12-2016 16:15:37 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12116763, 12114079, 12114080

NCMEC Note #1

ECD-LB 07-11-2016 20:43:20 UTC

Microsoft provided the following reported user information:

Screen Name: vt151234

IP Address: 24.91.154.58

Event Time Stamp: 6/1/2016 9:12:27 PM +00:00

NCMEC Note #2

ECD-KDS 07-12-2016 16:15:37 UTC

There are multiple reports on this target. Please see CT #12116763 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 07-12-2016 16:15:37 UTC

This concludes Section D

This concludes CyberTipline Report 12114081



CyberTipline Report 12116763

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-02-2016 17:55:53 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Section C: Additional Information Provided by NCMEC	4
NCMEC Note #1	4
NCMEC Note #2	4
Section D: Law Enforcement Contact Information	12
Vermont Office of Attorney General	12



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 01-01-0001 00:00:00 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
Peer to Peer Filenames: tmp5DA9 . jpg

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename:	tmp5DA9.jpg
Was File Reviewed by Company?	Yes
Child Pornography Categorization by ESP: (See Section B for further explanation)	A1
Original Binary Hash of File (PhotoDNA):	0,60,0,87,5,41,3,82,47,55,48,60,173,58,119,45,23,76,34,67,47,1,0,79,1,5 2,0,85,61,23,17,84,126,25,100,53,140,117,111,137,17,164,11,113,58,2,0, 85,1,29,2,36,97,8,25,32,140,24,108,38,74,130,130,71,13,147,25,41,43,3, 7,32,20,8,26,2,130,0,81,0,255,33,137,57,53,245,159,92,2,146,122,7,21,2 3,36,2,33,11,108,0,191,2,131,0,101,43,98,23,67,51,91,29,19,246,133,1,2 0,43,73,0,88,24,128,48,163,19,224,4,51,44,122,0,66,41,137,6,15,224,86, 22,21,32,96,0
Original URL Where File was Located:	D:\local\Temp\tmp5DA9.jpg

**Additional Information:****Where to serve legal process in Criminal Matters**

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other Online Services:

FAX: (425) 708-0096 Microsoft Corporation
Attn: Online Services Custodian of Records
One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	07-12-2016 16:15:31 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12116763, 12114079, 12114080, 12114081

NCMEC Note #1

ECD-LB 07-11-2016 20:43:57 UTC

Microsoft provided the following reported user information:

Screen Name: vt151234

IP Address: 24.91.154.58

Event Time Stamp: 6/1/2016 9:22:15 PM +00:00

NCMEC Note #2

ECD-KDS 07-12-2016 16:15:31 UTC

I reviewed the uploaded file and found what appears to be child pornography.

=====

CT/TA search results for: *vt151234*

12114079

12114080

12114081

12469964 VT

12469962 VT

12469960 VT

12469951 VT

12468566 VT

12468560 VT

12415755 VT

12415578 VT

12415511 VT

12415510 VT



11614028 VT

The above-listed reports were submitted by the reporting ESP and appear to regard the reported user. These reports appear to match the reported screen name. All reports were provided to the Vermont Office of Attorney General.

CT/TA search results for: 24.91.154.58

12114079
12114080
12114081
12766078 VT
12765579 VT
12765571 VT
12651701 VT
12651697 VT
12651690 VT
12627589 VT
12627584 VT
12627552 VT
12527760 VT
12527752 VT
12526159 VT
12526157 VT
12526156 VT
12526155 VT
12526153 VT
12526152 VT
12526151 VT
12526150 VT
12526149 VT
12469964 VT
12469962 VT
12469960 VT
12469951 VT
12468566 VT
12468560 VT
12415755 VT
12415578 VT
12415511 VT
12415510 VT
12051925 VT
12051516 VT
12050739 VT
12050735 VT
12050728 VT
12045016 VT
11855790 VT
11751259 VT
11751258 VT
11614028 VT

The above-listed reports were submitted by the reporting ESP and appear to regard the reported user. These reports appear to match



the reported IP address and appear to regard a similar reported screen name. All reports were provided to the Vermont Office of Attorney General.

CT reports 12114079, 12114080 and 12114081 were submitted by the reporting ESP and appear to regard the reported user. These reports appear to match the reported user name and the reported IP address. CT reports 12114079, 12114080 and 12114081 have been grouped with this report.

=====

WHOIS search results for: 24.91.154.58

Address lookup

canonical name

c-24-91-154-58 . hsd1 . vt . comcast.net .

aliases

addresses

24.91.154.58

Network Whois record

Queried whois.arin.net with "n ! NET-24-91-128-0-1 "...

NetRange: 24.91.128.0 - 24.91.255.255

CIDR: 24.91.128.0/17

NetName: NEW-ENGLAND-7

NetHandle: NET-24-91-128-0-1

Parent: RW2-NORTHEAST-2 (NET-24-91-0-0-1)

NetType: Reassigned

OriginAS:

Customer: Comcast Cable Communications Holdings, Inc (C02610697)

RegDate: 2010-10-18

Updated: 2010-10-18

Ref: <https://whois.arin.net/rest/net/NET-24-91-128-0-1>

CustName: Comcast Cable Communications Holdings, Inc

Address: 1800 Bishops Gate Blvd

City: Mt Laurel

StateProv: NJ

PostalCode: 08054

Country: US

RegDate: 2010-10-18

Updated: 2011-03-19

Ref: <https://whois.arin.net/rest/customer/C02610697>

OrgTechHandle: IC161-ARIN

OrgTechName: Comcast Cable Communications Inc

OrgTechPhone: +1-856-317-7200

OrgTechEmail: CNIPEO-lp-registration@comcast.com

OrgTechRef: <https://whois.arin.net/rest/poc/IC161-ARIN>

OrgAbuseHandle: NAPO-ARIN

OrgAbuseName: Network Abuse and Policy Observance

OrgAbusePhone: +1-888-565-4329

OrgAbuseEmail: abuse@comcast.net

OrgAbuseRef: <https://whois.arin.net/rest/poc/NAPO-ARIN>



DNS records

```

name class type data time to live
c-24-91-154-58.hsd1.vt.comcast.net IN A 24.91.154.58 7200s (02:00:00)
hsd1.vt.comcast.net IN NS dns105.comcast.net 7200s (02:00:00)
hsd1.vt.comcast.net IN NS dns103.comcast.net 7200s (02:00:00)
hsd1.vt.comcast.net IN NS dns102.comcast.net 7200s (02:00:00)
hsd1.vt.comcast.net IN NS dns101.comcast.net 7200s (02:00:00)
hsd1.vt.comcast.net IN NS dns104.comcast.net 7200s (02:00:00)
hsd1.vt.comcast.net IN SOA server: dns101.comcast.net email: dnsadmin@comcast.net serial: 1352080 refresh: 7200
retry: 3600 expire: 604800 minimum ttl: 7200 7200s (02:00:00)
comcast.net IN A 69.252.80.75 30s (00:00:30)
comcast.net IN RRSIG type covered: A (1) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 30 (00:00:30) signature
expiration: 2016-07-19 00:23:38Z signature inception: 2016-07-11 21:18:38Z key tag: 44553 signer's name: comcast.net
signature:
(1024 bits) 9ED5ACC1AF915B1EBA5D84E9D786CCB8
072831218347B732B9B55CF96457F383
96DE5498EE6A4CCF1E8AA7494B39F383
F4DFC0122FACE23C33670CC0713747A1
3113D337D3EA9EC71AC854D8C1B93F00
E01F79D05007B302E05B4341BAC56176
7E74833F580FA3FB867F1318DF8B2675
AEBF47D87EA366763FBA3DDB1619B4B7 30s (00:00:30)
comcast.net IN MX preference: 5 exchange: mx1.comcast.net 7200s (02:00:00)
comcast.net IN MX preference: 5 exchange: mx2.comcast.net 7200s (02:00:00)
comcast.net IN RRSIG type covered: MX (15) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 7200 (02:00:00) signature
expiration: 2016-07-19 00:23:38Z signature inception: 2016-07-11 21:18:38Z key tag: 44553 signer's name: comcast.net
signature:
(1024 bits) A590A3EEF79D530F5B5A981628E7F4A1
8D3E46D650A85A868F52C0520D1303C5
F68A2D121AA4EC42BFA4E70488A9D971
4AAB262A40C2583B69EC889799CF36E9
CB7FFD8C0C2F3C2C8716975A08711695
E2FE7F8466C0C8FB419098DE9FE24AA3
FCB2BE802B3B8B2837C3B2495F9E01E7
31534B83295FFDB47F3AE8401F2FE001 7200s (02:00:00)
comcast.net IN NS dns105.comcast.net 7200s (02:00:00)
comcast.net IN NS dns102.comcast.net 7200s (02:00:00)
comcast.net IN NS dns101.comcast.net 7200s (02:00:00)
comcast.net IN NS dns103.comcast.net 7200s (02:00:00)
comcast.net IN NS dns104.comcast.net 7200s (02:00:00)
comcast.net IN RRSIG type covered: NS (2) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 7200 (02:00:00) signature
expiration: 2016-07-19 00:23:38Z signature inception: 2016-07-11 21:18:38Z key tag: 44553 signer's name: comcast.net
signature:
(1024 bits) 274EEF735DACA1B3E90F4493A7B159C1
C3DE5E8EB9BB9157925A6A1C4BB6DC69
2A2DF82EBBDD9330E0EEBAC1ABD4BCF5
350656C00B9EDF6BF7FA85DE730BCBD7
DF9CA6149DECEB84F4D6AAEE12E5064D
ABAD068AE26FF3A9E4816E1DFA2206C1
82B519E68D64E84EA40C102F3A3D2528
011A7D1BC7012DEAFDA90A324F90C6AF 7200s (02:00:00)

```



comcast.net IN TXT v=spf1 ip4:96.114.154.128/25 ip4:69.252.207.0/25 include:_spf6.comcast.net include:_spf.mdp.comcast.net ?all 7200s (02:00:00)

comcast.net IN RRSIG type covered: TXT (16) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 7200 (02:00:00) signature expiration: 2016-07-19 00:23:38Z signature inception: 2016-07-11 21:18:38Z key tag: 44553 signer's name: comcast.net signature:

(1024 bits) 69B28D2291B551C11672F983EB8A9921

2267A3FE745A94ADD06615F33B716409

762BF200BEB935DFB78B24B5C76D38DB

2926BB3893F2AA722878E73EA0EF7377

650196B1B19E684DA2092F46F31D502B

4EDF158D9E908780AB1C2CEA5CAA1253

B5CDC76D9625EDCFAF4871D9FBE91A67

3C2F0C2FE280EEA4692D4A641B5B11AC 7200s (02:00:00)

comcast.net IN NSEC next domain name: 4gmobile.comcast.net record types: A NS SOA MX TXT RRSIG NSEC DNSKEY 3600s (01:00:00)

comcast.net IN RRSIG type covered: NSEC (47) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 3600 (01:00:00) signature expiration: 2016-07-19 00:23:38Z signature inception: 2016-07-11 21:18:38Z key tag: 44553 signer's name: comcast.net signature:

(1024 bits) C5DC6F820244B18AA6E8BDBA6CA04E09

5CE14F18190610A5150801200552E061

999F2E8AB453C2064A2C87BF753D5D03

7159D7F046A9A71806BF4C0D50D42949

1B605C2D8C0ACD2775F7D7DCEC9AAB92

E6AD7893E872DC5965C526B2B6AAF605

8C7FE50C69711802297D85156E08B419

0F53DD8C401A8630CAC8E81241D509EC 3600s (01:00:00)

comcast.net IN DNSKEY flags: SecureEntryPoint, ZoneKey (257) protocol: 3 algorithm: RSA/SHA-1 (5) public key: (2080 bits) 03010001C753C17B8A204454A0468E1C

211A7CF0A01D6F03ABC39FB433C3D6C6

42C02507ED58DF49742982F918506FBA

14DF4834FDAE1F26F345EFE6E041BC1C

3F3390AB5A201CEB61921C6DC86E5CA6

796E2C248F58483131A50C6D230F48F7

AE3889924DDD0E4CA02AF57C16CC0426

8F57EFE0966ED7F858A817AA777FD897

2C9620CAE17BA316CC36EDE5A95E51D9

B794AE41BD0DD6398C6B31125F060962

D19771EE6F8B8A4186513D3948024259

313F179DBDA7A54F984AC583F79481F8

BE306B28CCD013B3B3A01E253AC25585

BBC31755595330BA9F8DB0F165AF8C10

D8DD38A53AFB02F497BB0CE0F7C90960

726890F343CCE339277D027BE803F162

BAE8C131 3600s (01:00:00)

comcast.net IN DNSKEY flags: ZoneKey (256) protocol: 3 algorithm: RSA/SHA-1 (5) public key: (1056 bits) 03010001CA97AA33D8252C366DFEFC49

7CF723676A27CC98507CC103DB63E7D3

6BC5386CB117903AA8C30556F0722F9C

C8878AEF6A0CB46EE2C4392A1EECB1F1

75DA4A5E1697D475A8302109DF494861

1ED85D247B70F917CA36DBF0085118A7

957D15F56555E71972CEA2C9DE89FE46

071354117F189DECCE98DEBAE6697E95



B72D858B 3600s (01:00:00)

comcast.net IN RRSIG type covered: DNSKEY (48) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 3600 (01:00:00)
signature expiration: 2016-10-18 21:23:38Z signature inception: 2016-06-20 17:23:38Z key tag: 40909 signer's name:

comcast.net signature:

(2048 bits) 336FDBCBA74E9D0D5950E01A3435157B

8637A8500996E54C9F769EBE7F7739B3

42B8D1595E054A80AD43D1F4D8A493EE

F32DA95BD957ADD42C1C1E5DB7B463CA

6E8184313CDE119686306398C384BD77

724B665A659B709C691FC8588372031D

D362D25FDF5336B193D510B6F1E9BA28

A67569FB3BF0A7A32D36B84BE96FADE7

B8B1FAA73D14085A46E42C5C29682687

D32C5729F7A72BA01DDB01AC8DE96963

28FB42E7ADB3C38C797465782629D299

69997B123420DDF7DAE46CA0707AAE05

B1274FBD835000F7A905989685AC5C0E

87B15C7D0D09B4CA5CA0A94B9F5D3D23

9271134B64803762B385B149034F856C

A31C7E8699ED8236AA774C23094E5A38 3600s (01:00:00)

comcast.net IN RRSIG type covered: DNSKEY (48) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 3600 (01:00:00)
signature expiration: 2016-07-19 00:23:38Z signature inception: 2016-07-11 21:18:38Z key tag: 44553 signer's name:

comcast.net signature:

(1024 bits) 6E40BF1A105428FD960EC11A236B7481

4CACCE84F99262B30AEA1B0543A390B4

49E939BCEAC603FC27C72DAD1D619BAA

1C442C3F6D75EB6A27D79211F3920305

1CEA225B18E90216F0A4A61C5E71605F

2ED9E94696C74E832AB9C1441F5C28BE

93BCEBEB6D3E112873B611D8B2F7D8F3

20B07E0317F03207A5BBD2B832FFCEA1 3600s (01:00:00)

comcast.net IN SOA server: dns101.comcast.net email: domregtech@comcastonline.com serial: 2008189013 refresh: 7200
retry: 3600 expire: 1209600 minimum ttl: 3600 7200s (02:00:00)

comcast.net IN RRSIG type covered: SOA (6) algorithm: RSA/SHA-1 (5) labels: 2 original ttl: 7200 (02:00:00) signature
expiration: 2016-07-19 00:23:38Z signature inception: 2016-07-11 21:18:38Z key tag: 44553 signer's name: comcast.net
signature:

(1024 bits) 2E36B5169304B884F2810B9D88D62CEC

D848D852271C97314A90155A8C9F739B

D6E05C9BB8327F3544D63449B222121A

3FC09D591F2673234C554759ADD8A3A9

CA92875EFBF64AAE9483767B9DE53949

D6FF893468895EDAD9B110A8F8DA18BC

F10C36D23971D91E96720513C9F27D83

0399A203749AD8B6298B20B0F99C8BF4 7200s (02:00:00)

58.154.91.24.in-addr.arpa IN PTR c-24-91-154-58.hsd1.vt.comcast.net 7200s (02:00:00)

154.91.24.in-addr.arpa IN NS dns102.comcast.net 7200s (02:00:00)

154.91.24.in-addr.arpa IN NS dns103.comcast.net 7200s (02:00:00)

154.91.24.in-addr.arpa IN NS dns104.comcast.net 7200s (02:00:00)

154.91.24.in-addr.arpa IN NS dns105.comcast.net 7200s (02:00:00)

154.91.24.in-addr.arpa IN NS dns101.comcast.net 7200s (02:00:00)

154.91.24.in-addr.arpa IN SOA server: dns101.comcast.net email: dnsadmin@comcast.net serial: 2139 refresh: 7200
retry: 3600 expire: 604800 minimum ttl: 7200 7200s (02:00:00)



Traceroute

Tracing route to c-24-91-154-58.hsd1.vt.comcast.net [24.91.154.58] ...

	hop	rtt	rtt	rtt	ip address	fully qualified domain name
1	1	0	0		208.101.16.73	49.10.65d0.ip4.static.sl-reverse.com
2	1	0	0		66.228.118.153	ae11.dar01.sr01.dal01.networklayer.com
3	0	0	0		173.192.18.210	ae6.bbr01.eq01.dal03.networklayer.com
4	1	0	5		75.149.228.33	be-111-pe03.1950stemmons.tx.ibone.comcast.net
5	1	2	2		68.86.86.173	hu-0-4-0-1-cr02.dallas.tx.ibone.comcast.net
6	16	14	14		68.86.84.229	be-11724-cr02.denver.co.ibone.comcast.net
7	29	29	29		68.86.85.169	be-10517-cr02.350ecermak.il.ibone.comcast.net
8	58	58	58		68.86.91.6	be-7922-ar01.woburn.ma.boston.comcast.net
9	62	62	62		162.151.113.14	
10	61	61	60		68.85.143.46	te-3-0-0-ten02.bennington.vt.boston.comcast.net
11	*	*	*			
12	*	*	*			
13	*	*	*			
14	*	*	*			

Trace aborted

===

Country: US
 Region: VT
 City: Bennington
 Postal Code: 05201
 Latitude: 42.8626
 Longitude: -73.0998
 Metropolitan Code: Albany-Schenectady-Troy
 ISP: Comcast Cable
 Organization: Comcast Cable

===

Country: US
 Region: VT
 City: Bennington
 Postal Code: 05201
 Latitude: 42.8781345
 Longitude: -73.1967741
 Area: 12.507 sq. km. (4.829 sq. miles)

=====

Based on the WHOiS results, I will place this report on the VPN for Vermont.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.



For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 07-12-2016 16:15:31 UTC

This concludes Section D

This concludes CyberTipline Report 12116763



CyberTipline Report 12415510

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-13-2016 18:09:08 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-11-2016 07:07:53 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp4080.jpg

User or Person Being Reported

Screen/User Name: jvt1512345,4d19a1fabfa401bd
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp4080.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A1
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

6,34,24,3,27,40,39,20,3,23,4,10,16,53,30,30,51,86,54,154,117,223,252,9
 4,3,93,13,88,16,78,18,231,55,16,9,210,79,107,47,169,61,102,92,75,111,2
 19,67,171,38,83,27,153,35,123,109,96,30,65,87,92,78,36,19,179,57,48,5
 7,192,13,97,74,159,27,33,17,74,71,39,43,114,50,102,66,103,34,99,102,5
 2,84,27,63,115,54,74,88,75,66,10,29,52,32,51,59,51,66,44,82,100,71,80,
 96,109,40,88,86,58,52,105,25,120,46,25,78,35,22,54,71,79,18,41,41,90,1
 8,31,19,122,19,67,16,141,5,80,15,88

Original URL Where File was Located:

D:\local\Temp\tmp4080.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
 Online Services:

FAX: (425) 708-0096 Microsoft Corporation

Attn: Online Services Custodian of Records

One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12415510



CyberTipline Report 12415511

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-13-2016 18:09:08 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*

Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-11-2016 07:09:51 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp40B0.jpg

User or Person Being Reported

Screen/User Name: jvt1512345,4d19a1fabfa401bd
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp40B0.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A1
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

26,75,0,155,48,46,0,122,29,112,15,177,96,8,10,114,18,42,0,52,23,18,6,3
 8,42,225,18,131,77,27,0,225,58,37,18,151,112,22,26,105,34,92,4,157,79,
 14,1,123,5,255,119,7,21,33,28,28,22,10,13,70,148,30,16,130,61,162,55,9
 3,182,19,24,38,0,215,140,19,3,162,67,23,9,24,31,40,71,5,25,73,96,77,52,
 75,130,22,66,20,0,255,4,79,4,150,15,51,22,42,47,16,59,32,42,24,170,1,5
 8,15,68,8,149,2,3,255,19,71,14,57,44,38,42,30,67,43,36,42,66,22,200,1,3
 8,9,106,3,49,4

Original URL Where File was Located:

D:\local\Temp\tmp40B0.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
 Online Services:

FAX: (425) 708-0096 Microsoft Corporation
 Attn: Online Services Custodian of Records
 One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12415511



CyberTipline Report 12415578

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-13-2016 18:09:15 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-11-2016 23:57:51 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp5AA4.jpg

User or Person Being Reported

Screen/User Name: jvt1512345,4d19a1fabfa401bd
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp5AA4.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A2
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

7,85,1,24,95,6,5,31,84,6,35,3,5,62,7,21,0,236,0,61,123,145,2,38,8,120,3,10,156,14,8,19,124,36,34,28,14,113,35,27,26,253,166,47,77,101,255,27,5,119,3,12,162,19,6,14,133,49,29,56,62,78,72,28,137,64,173,21,107,63,255,38,3,101,29,1,154,17,30,3,137,55,48,33,95,30,70,26,151,21,146,54,150,16,179,118,1,82,59,0,113,26,57,7,114,49,15,65,186,20,64,27,45,51,85,49,60,13,53,129,1,75,50,0,65,41,52,3,96,92,7,58,255,27,22,67,49,56,70,17,43,28,85,10

Original URL Where File was Located:

D:\local\Temp\tmp5AA4.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other Online Services:

FAX: (425) 708-0096 Microsoft Corporation

Attn: Online Services Custodian of Records

One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A2: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12415578



CyberTipline Report 12415755

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-13-2016 18:13:41 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-13-2016 00:56:51 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp6AE2.jpg

User or Person Being Reported

Screen/User Name: jvt1512345,4d19a1fabfa401bd
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp6AE2.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A1
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

26,75,0,155,48,46,0,122,29,112,15,177,96,8,10,114,18,42,0,52,23,18,6,3
 8,42,225,18,131,77,27,0,225,58,37,18,151,112,22,26,105,34,92,4,157,79,
 14,1,123,5,255,119,7,21,33,28,28,22,10,13,70,148,30,16,130,61,162,55,9
 3,182,19,24,38,0,215,140,19,3,162,67,23,9,24,31,40,71,5,25,73,96,77,52,
 75,130,22,66,20,0,255,4,79,4,150,15,51,22,42,47,16,59,32,42,24,170,1,5
 8,15,68,8,149,2,3,255,19,71,14,57,44,38,42,30,67,43,36,42,66,22,200,1,3
 8,9,106,3,49,4

Original URL Where File was Located:

D:\local\Temp\tmp6AE2.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
 Online Services:

FAX: (425) 708-0096 Microsoft Corporation

Attn: Online Services Custodian of Records

One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	---------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12415755



CyberTipline Report 12468560

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-15-2016 16:23:16 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-15-2016 00:37:22 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp6B94.jpg

User or Person Being Reported

Screen/User Name: jvt15123456
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp6B94.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A1
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

10,145,3,86,20,19,3,74,29,18,4,86,142,28,11,157,104,5,13,78,5,10,7,13,7
 ,103,7,96,22,35,3,137,44,20,1,128,137,26,34,120,208,13,33,150,31,6,1,3
 3,34,99,106,24,11,80,98,23,46,20,48,32,127,23,52,71,159,28,54,193,111,
 2,15,162,80,42,35,111,24,81,73,34,35,49,86,21,44,110,41,89,133,26,63,1
 08,244,3,71,56,84,12,11,195,76,29,11,232,42,31,7,148,56,77,39,73,233,5
 8,120,33,186,55,26,75,19,45,51,19,39,10,25,53,40,10,3,77,70,22,7,103,2
 36,86,5,131,38,124,4,167

Original URL Where File was Located:

D:\local\Temp\tmp6B94.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
 Online Services:

FAX: (425) 708-0096 Microsoft Corporation
 Attn: Online Services Custodian of Records
 One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	---------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12468560



CyberTipline Report 12468566

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-15-2016 16:23:16 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-15-2016 00:25:33 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp6BA4.jpg

User or Person Being Reported

Screen/User Name: jvt15123456
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp6BA4.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A2
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

23,73,27,131,36,72,63,78,27,30,52,29,18,58,53,27,46,65,37,105,113,14,6
 ,235,43,46,83,113,67,37,98,95,35,118,51,92,80,73,65,96,34,235,44,148,7
 9,36,0,95,63,38,19,121,88,53,20,125,21,104,32,126,74,127,23,157,47,15
 9,21,82,30,47,15,32,45,47,41,84,61,54,32,154,33,68,26,141,36,106,30,10
 2,109,79,69,18,23,62,75,1,43,113,75,51,34,69,78,64,56,37,133,44,91,38,
 193,18,115,44,192,8,38,50,175,4,64,123,134,47,85,20,254,8,58,14,219,3,
 44,16,157,0,33,20,118,1,36,12,102,1

Original URL Where File was Located:

D:\local\Temp\tmp6BA4.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
 Online Services:

FAX: (425) 708-0096 Microsoft Corporation

Attn: Online Services Custodian of Records

One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A2: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12468566



CyberTipline Report 12469951

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-15-2016 17:14:04 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-15-2016 00:34:56 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmpF347.jpg

User or Person Being Reported

Screen/User Name: jvt15123456
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmpF347.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: B2
(See Section B for further explanation)



Original Binary Hash of File (PhotoDNA): 53,18,0,97,108,90,63,119,44,56,131,21,22,35,117,17,84,55,71,88,11,45,0,102,19,42,0,84,174,11,14,149,75,75,41,77,33,58,28,62,7,115,8,139,36,7,0,86,6,84,1,40,128,6,0,112,107,22,8,148,18,110,9,130,12,110,0,115,100,0,0,52,0,134,28,5,57,36,4,72,144,21,7,98,19,142,2,118,40,53,4,68,143,0,14,10,0,202,103,0,34,110,50,13,223,46,51,19,33,234,40,33,123,19,45,18,171,0,82,0,0,209,132,2,24,134,130,0,189,48,75,21,32,200,84,18,138,11,125,0,209,0,139,0

Original URL Where File was Located: D:\local\Temp\tmpF347.jpg

Additional Information: Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other Online Services:
 FAX: (425) 708-0096 Microsoft Corporation
 Attn: Online Services Custodian of Records
 One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS
 Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT
 Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

B2: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12469951



CyberTipline Report 12469960

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-15-2016 17:14:30 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-15-2016 00:48:13 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp55FB.jpg

User or Person Being Reported

Screen/User Name: jvt15123456
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp55FB.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A1
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

33,20,20,95,55,51,7,120,7,68,16,61,58,10,20,71,36,50,17,105,5,63,14,12
 3,23,24,78,67,34,11,63,74,58,27,55,28,58,50,84,19,15,48,76,40,18,34,12
 3,33,111,19,69,152,45,38,118,148,70,50,88,73,38,96,33,150,49,39,45,18
 6,47,97,49,176,56,71,141,62,119,52,79,131,118,77,49,61,15,139,79,40,6
 0,71,66,79,35,101,34,103,147,65,103,66,113,219,127,33,173,45,52,17,33
 ,163,99,52,41,112,117,53,63,37,130,11,93,13,78,9,117,175,118,8,129,80,
 125,15,70,149,152,91,103,62,227,8,7,67,92,0

Original URL Where File was Located:

D:\local\Temp\tmp55FB.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
 Online Services:

FAX: (425) 708-0096 Microsoft Corporation
 Attn: Online Services Custodian of Records
 One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	---------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12469960



CyberTipline Report 12469962

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-15-2016 17:14:37 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-15-2016 01:03:03 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp7348.jpg

User or Person Being Reported

Screen/User Name: jvt15123456
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp7348.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A2
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

11,24,58,5,27,12,34,0,154,20,100,4,59,40,53,26,61,110,68,20,0,118,55,0,
 17,45,47,2,111,35,104,1,159,39,136,6,58,47,133,9,55,95,128,5,0,173,105
 ,4,21,72,114,23,181,37,138,34,127,67,101,62,67,31,79,84,35,76,59,28,0,
 231,76,57,99,48,74,90,117,29,131,95,60,182,96,145,192,48,107,161,73,8
 3,37,49,0,168,98,56,28,34,73,45,77,17,50,119,50,59,87,163,61,16,111,17
 5,27,76,50,214,20,66,92,138,2,35,37,52,28,18,69,37,35,39,115,18,40,32,
 144,26,55,6,180,23,35,10,146,13

Original URL Where File was Located:

D:\local\Temp\tmp7348.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
 Online Services:

FAX: (425) 708-0096 Microsoft Corporation
 Attn: Online Services Custodian of Records
 One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A2: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	---------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12469962



CyberTipline Report 12469964

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-15-2016 17:14:47 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-15-2016 01:07:12 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp9885.jpg

User or Person Being Reported

Screen/User Name: jvt15123456
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp9885.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A1
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

23,18,52,118,45,37,52,116,60,93,95,40,13,106,255,5,5,81,149,0,2,11,32,
1,56,60,59,211,33,84,36,255,110,26,15,255,92,64,50,115,18,190,85,40,2,
21,92,1,10,144,71,95,34,66,69,101,119,29,51,103,98,64,28,214,130,36,6
2,174,47,9,133,126,2,91,31,85,23,33,42,46,49,29,92,47,48,39,77,36,37,6
6,18,131,90,20,12,211,2,30,19,72,32,28,16,100,80,17,52,187,35,116,33,1
71,51,64,31,103,83,11,69,61,10,33,9,49,30,38,35,42,77,33,138,41,36,121
,84,50,52,34,6,99,36,0,2,95

Original URL Where File was Located:

D:\local\Temp\tmp9885.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
Online Services:

FAX: (425) 708-0096 Microsoft Corporation
Attn: Online Services Custodian of Records
One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	---------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12469964



CyberTipline Report 12526149

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-17-2016 16:51:46 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-17-2016 01:33:00 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp367E.jpg

User or Person Being Reported

Screen/User Name: jvt1234515
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp367E.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A1
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

0,139,93,64,3,74,18,47,9,33,19,16,66,22,82,6,91,21,182,28,25,74,152,12,
0,212,15,71,5,47,12,36,80,8,33,20,146,58,138,65,74,58,51,131,128,63,77,
,81,3,191,56,29,12,61,62,10,122,28,22,47,108,221,31,144,198,53,38,147,
182,6,86,45,8,130,37,34,28,119,43,24,66,78,23,77,91,122,72,85,198,71,7
1,84,181,26,32,101,16,156,75,17,51,118,58,30,83,93,118,11,83,90,108,2
1,115,53,113,21,180,75,71,54,26,83,25,152,32,66,20,109,44,41,45,136,6
2,40,40,94,43,42,46,48,96,27,18,64

Original URL Where File was Located:

D:\local\Temp\tmp367E.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
Online Services:

FAX: (425) 708-0096 Microsoft Corporation
Attn: Online Services Custodian of Records
One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	---------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12766078, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12526149



CyberTipline Report 12526150

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-17-2016 16:51:46 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-17-2016 00:41:25 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp36FD.jpg

User or Person Being Reported

Screen/User Name: jvt1234515
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp36FD.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A1
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

5,127,1,139,38,108,5,241,56,86,18,159,28,19,14,195,159,23,69,77,16,54,78,7,10,216,8,144,92,104,38,110,117,46,43,63,90,30,99,33,169,47,87,124,70,28,58,152,40,61,20,122,73,34,50,68,62,54,22,130,181,42,31,108,36,119,40,189,80,29,13,194,22,104,57,53,60,34,28,91,96,19,69,73,97,58,58,108,13,104,36,131,51,18,19,81,26,99,83,28,17,84,49,42,66,20,29,142,92,60,43,122,32,113,130,140,104,28,83,104,88,47,33,41,1,103,42,23,51,14,74,20,85,60,54,36,49,51,52,102,58,99,109,70

Original URL Where File was Located:

D:\local\Temp\tmp36FD.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other Online Services:

FAX: (425) 708-0096 Microsoft Corporation

Attn: Online Services Custodian of Records

One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12526150



CyberTipline Report 12526151

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-17-2016 16:51:46 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-17-2016 01:24:01 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp37AB.jpg

User or Person Being Reported

Screen/User Name: jvt1234515
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp37AB.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A1
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

0,50,3,66,0,63,0,128,34,11,0,157,17,24,3,139,39,12,1,150,52,8,4,57,0,74,
0,66,0,90,6,68,54,18,18,63,46,66,14,64,51,32,15,80,123,0,2,82,0,59,16,1
3,16,41,65,6,43,17,116,25,20,47,98,41,15,29,56,9,74,1,14,18,35,17,98,14
,61,101,180,40,40,137,80,166,66,58,71,191,69,33,90,59,63,13,50,14,105,
59,71,107,27,197,37,255,13,128,44,160,154,55,126,100,63,78,89,232,10
2,23,17,179,11,160,79,55,6,120,169,82,103,9,199,15,129,107,185,25,25,
106,148,23,26,39,201,34

Original URL Where File was Located:

D:\local\Temp\tmp37AB.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
Online Services:

FAX: (425) 708-0096 Microsoft Corporation
Attn: Online Services Custodian of Records
One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12526151



CyberTipline Report 12526152

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-17-2016 16:51:46 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*

Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-17-2016 01:24:29 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp375C.jpg

User or Person Being Reported

Screen/User Name: jvt1234515
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp375C.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A1
(See Section B for further explanation)



Original Binary Hash of File (PhotoDNA): 0,72,0,74,7,67,0,111,49,31,7,96,17,65,6,97,135,2,0,159,114,0,0,80,0,82,1,29,10,81,26,30,83,29,28,38,17,92,41,28,113,5,32,28,163,0,4,53,0,65,33,2,26,30,83,0,56,84,107,23,37,48,46,42,71,9,53,8,102,1,26,18,21,97,69,10,3,108,22,134,105,62,219,116,70,75,76,117,94,111,51,98,79,80,21,19,62,19,207,182,83,144,52,124,159,55,226,30,196,109,76,38,222,101,94,56,2,38,161,17,43,66,3,79,83,19,10,128,76,32,3,167,57,33,10,36,51,13,157,2,118,38,118,28,137,18

Original URL Where File was Located: D:\local\Temp\tmp375C.jpg

Additional Information: Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other Online Services:
 FAX: (425) 708-0096 Microsoft Corporation
 Attn: Online Services Custodian of Records
 One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS
 Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT
 Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12526152



CyberTipline Report 12526153

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-17-2016 16:51:46 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-17-2016 00:51:50 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp38E4.jpg

User or Person Being Reported

Screen/User Name: jvt1234515
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp38E4.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A1
(See Section B for further explanation)



Original Binary Hash of File (PhotoDNA): 4,112,210,32,16,65,132,23,27,16,92,3,150,9,170,35,104,61,220,55,46,57,199,31,2,208,27,101,11,55,29,64,47,24,21,67,140,93,37,151,135,46,13,205,50,90,18,175,50,160,28,51,26,153,37,68,69,54,32,107,102,96,33,92,133,38,26,91,111,13,68,37,72,85,42,31,21,159,39,25,112,29,109,18,46,137,95,19,208,21,64,33,175,2,113,33,75,47,21,35,22,140,46,16,83,29,19,51,81,82,65,78,138,43,129,51,72,54,47,153,37,17,6,33,16,93,29,29,29,41,16,23,52,8,9,33,117,21,31,87,41,114,67,74

Original URL Where File was Located: D:\local\Temp\tmp38E4.jpg

Additional Information: Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other Online Services:
 FAX: (425) 708-0096 Microsoft Corporation
 Attn: Online Services Custodian of Records
 One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS
 Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT
 Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12526153



CyberTipline Report 12526155

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-17-2016 16:51:47 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-17-2016 01:01:26 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp3AF9.jpg

User or Person Being Reported

Screen/User Name: jvt1234515
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp3AF9.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A1
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

25,57,14,63,107,40,21,67,130,87,28,95,76,29,35,68,24,33,34,24,26,46,74
 ,31,45,149,93,49,51,38,34,53,139,33,39,58,89,9,41,35,85,6,65,14,61,50,9
 3,14,53,213,68,12,52,66,95,2,108,54,51,61,137,4,24,90,49,14,10,78,119,
 2,10,56,67,175,74,4,136,138,98,62,87,148,109,73,98,16,64,46,92,32,42,7
 5,167,1,43,20,92,201,55,70,108,203,64,151,162,90,96,105,96,28,66,29,1
 15,58,106,17,120,46,34,67,115,67,38,106,72,102,206,59,96,117,62,53,17
 1,5,25,14,68,66,98,43,20,201,17,181

Original URL Where File was Located:

D:\local\Temp\tmp3AF9.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
 Online Services:

FAX: (425) 708-0096 Microsoft Corporation

Attn: Online Services Custodian of Records

One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12526155



CyberTipline Report 12526156

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-17-2016 16:51:47 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-17-2016 00:44:33 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp3B38.jpg

User or Person Being Reported

Screen/User Name: jvt1234515
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp3B38.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A1
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

2,132,92,5,15,107,119,2,106,5,138,2,68,27,234,17,90,79,163,61,63,37,50
 ,73,23,90,32,65,38,69,109,18,65,26,100,35,38,98,28,157,111,97,17,162,1
 74,17,46,57,114,33,17,115,69,51,48,99,24,101,26,111,73,121,87,101,95,
 146,77,96,255,6,9,155,66,22,17,100,111,106,86,188,73,96,37,132,97,62,
 56,101,46,155,89,61,235,54,35,101,20,23,62,78,46,41,30,134,44,39,12,9
 8,31,28,23,148,43,36,45,139,120,26,60,34,19,34,59,59,24,38,92,12,22,40
 ,98,16,35,14,84,17,58,10,87,30,81,12,49,27

Original URL Where File was Located:

D:\local\Temp\tmp3B38.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
 Online Services:

FAX: (425) 708-0096 Microsoft Corporation
 Attn: Online Services Custodian of Records
 One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12526156



CyberTipline Report 12526157

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-17-2016 16:51:47 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*

Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-17-2016 01:23:30 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp3B49.jpg

User or Person Being Reported

Screen/User Name: jvt1234515
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp3B49.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A1
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

0,28,14,13,37,10,18,24,133,57,40,33,60,101,27,97,51,57,28,90,22,4,0,22,
0,56,69,45,32,42,45,108,109,90,25,194,51,99,35,139,83,50,26,94,49,1,7,
14,0,135,2,128,3,121,1,174,64,28,5,206,51,70,14,179,163,15,10,196,115,
1,6,72,0,126,15,34,11,81,71,19,59,19,139,14,36,71,101,21,108,20,71,30,
176,0,12,63,4,65,101,6,78,53,188,23,73,128,165,181,62,87,111,162,80,4
4,120,52,82,14,46,39,33,61,64,70,50,120,46,118,25,201,48,144,101,43,8
2,138,162,69,36,170,109,33,43,91

Original URL Where File was Located:

D:\local\Temp\tmp3B49.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
Online Services:

FAX: (425) 708-0096 Microsoft Corporation

Attn: Online Services Custodian of Records

One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	---------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12526157



CyberTipline Report 12526159

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-17-2016 16:51:47 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*

Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-17-2016 01:04:15 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp3E39.jpg

User or Person Being Reported

Screen/User Name: jvt1234515
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp3E39.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A1
(See Section B for further explanation)



Original Binary Hash of File (PhotoDNA): 0,185,0,27,6,154,5,56,31,109,63,37,151,14,15,67,84,0,1,30,80,0,10,6,0,2
26,2,14,7,192,19,37,19,85,26,75,131,13,14,49,161,8,18,27,105,20,13,63,
0,225,12,5,3,159,69,1,10,111,102,4,131,22,98,19,118,41,41,128,95,50,13
,110,0,200,33,4,10,136,38,14,46,69,94,18,119,47,184,9,47,164,147,36,52
,37,49,50,0,203,11,24,11,180,14,60,125,14,41,32,114,21,94,15,42,181,11
9,17,49,109,136,55,2,145,1,86,21,158,50,15,177,12,78,5,98,9,114,1,6,86,
137,9,10,95,129,35

Original URL Where File was Located: D:\local\Temp\tmp3E39.jpg

Additional Information: Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
Online Services:
FAX: (425) 708-0096 Microsoft Corporation
Attn: Online Services Custodian of Records
One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS
Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT
Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12526159



CyberTipline Report 12527752

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-17-2016 17:49:33 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*

Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-17-2016 01:10:36 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp2149.jpg

User or Person Being Reported

Screen/User Name: jvt1234515
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp2149.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A2
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

30,53,3,55,56,62,15,30,91,90,37,49,97,82,14,157,98,77,23,125,25,11,1,3
 9,90,13,3,92,79,42,13,46,61,92,31,53,85,49,48,56,48,44,27,43,36,4,3,34,
 48,10,8,32,113,74,32,64,98,104,28,125,97,72,85,122,52,43,21,64,32,3,0,
 32,39,13,64,4,99,159,37,41,140,125,17,122,133,151,53,239,131,44,23,11
 5,55,9,32,21,32,46,16,18,104,235,48,39,89,177,43,66,106,101,29,86,222,
 22,68,35,116,20,49,53,11,56,15,7,123,124,79,68,75,193,254,15,123,93,2
 12,8,201,45,132,27,63,60,68,30

Original URL Where File was Located:

D:\local\Temp\tmp2149.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
 Online Services:

FAX: (425) 708-0096 Microsoft Corporation
 Attn: Online Services Custodian of Records
 One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A2: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	---------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12527752



CyberTipline Report 12527760

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-17-2016 17:50:22 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*

Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-17-2016 01:27:11 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmpDF4A.jpg

User or Person Being Reported

Screen/User Name: jvt1234515
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmpDF4A.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: B1
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

17,89,23,109,40,83,11,255,43,89,10,163,87,25,5,235,112,8,2,124,15,17,5
 34,36,167,55,110,19,102,81,64,14,26,4,67,84,8,17,68,173,22,48,91,58,6,
 6,43,94,71,77,47,35,192,80,42,5,61,37,23,132,7,45,35,179,63,57,60,68,1
 6,21,22,27,76,78,94,20,133,66,109,15,61,66,11,61,21,79,26,117,36,38,14
 7,40,7,27,205,30,52,96,140,41,32,139,83,122,22,164,20,70,86,255,14,13,
 71,207,27,23,4,214,53,53,17,133,11,32,22,103,8,116,28,108,26,86,96,11
 3,26,15,79,80,15,29,13,41,26

Original URL Where File was Located:

D:\local\Temp\tmpDF4A.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
 Online Services:

FAX: (425) 708-0096 Microsoft Corporation
 Attn: Online Services Custodian of Records
 One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

B1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	---------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12527760



CyberTipline Report 12627552

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-21-2016 17:31:46 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*

Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-21-2016 00:57:01 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp3C6D.jpg

User or Person Being Reported

Screen/User Name: jvt12345615
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp3C6D.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A2
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

55,116,25,222,70,12,1,181,51,129,13,141,169,154,63,224,76,56,4,113,49,27,0,42,22,222,124,33,89,68,32,151,115,67,32,164,135,100,152,75,44,8,0,15,68,88,13,7,28,0,210,38,23,94,148,55,41,123,79,124,29,163,71,38,68,39,82,92,17,94,4,47,4,2,250,19,37,135,113,47,54,95,95,73,161,159,57,3,4,62,71,62,43,38,51,11,27,21,19,177,64,115,49,58,102,27,27,26,36,39,94,3,32,40,46,40,8,71,86,6,3,47,84,42,116,11,9,115,71,40,24,17,19,21,45,0,8,14,28,5,19,11,63,3,21,5

Original URL Where File was Located:

D:\local\Temp\tmp3C6D.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other Online Services:

FAX: (425) 708-0096 Microsoft Corporation

Attn: Online Services Custodian of Records

One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A2: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12627552



CyberTipline Report 12627584

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-21-2016 17:32:35 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*

Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-21-2016 01:34:27 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmpFB0C.jpg

User or Person Being Reported

Screen/User Name: jvt12345615
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmpFB0C.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A1
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

0,118,98,28,0,225,152,7,4,53,37,1,58,1,3,15,249,0,0,102,232,121,23,102,
3,61,3,103,16,155,88,65,1,140,133,10,33,26,59,5,171,6,6,65,255,92,8,89,
12,85,1,55,47,61,27,56,2,99,58,50,4,77,37,35,139,20,36,28,255,89,22,11
8,13,85,42,6,38,62,43,46,2,100,35,48,28,60,33,26,128,28,72,45,107,80,6
1,104,2,55,59,31,10,67,76,26,15,94,100,27,6,81,69,24,122,33,48,48,173,
52,135,66,13,52,6,227,108,45,43,196,18,120,20,124,19,37,8,61,106,12,6
5,7,176,5,84,7

Original URL Where File was Located:

D:\local\Temp\tmpFB0C.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
Online Services:

FAX: (425) 708-0096 Microsoft Corporation
Attn: Online Services Custodian of Records
One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12627584



CyberTipline Report 12627589

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-21-2016 17:32:48 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*

Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-21-2016 01:42:56 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp2E23.jpg

User or Person Being Reported

Screen/User Name: jvt12345615
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp2E23.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A1
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

23,7,10,23,25,6,11,47,18,7,4,36,29,2,9,20,26,7,13,2,30,5,6,6,27,51,7,54,4
 2,96,0,181,157,17,5,127,50,0,13,9,30,9,9,4,25,14,7,16,9,144,15,43,54,18
 2,10,116,255,18,1,147,134,1,3,114,28,12,5,24,12,87,10,81,22,177,65,7,1
 9,197,56,25,155,23,19,63,231,39,13,168,101,69,0,127,33,169,24,159,36,
 147,31,10,18,199,124,8,121,46,93,14,116,86,100,68,103,111,18,202,223,
 58,90,74,49,69,14,57,26,139,92,16,92,60,174,25,30,84,82,55,35,76,9,50,
 255,9,14,62

Original URL Where File was Located:

D:\local\Temp\tmp2E23.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
 Online Services:

FAX: (425) 708-0096 Microsoft Corporation
 Attn: Online Services Custodian of Records
 One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	---------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12627589



CyberTipline Report 12651690

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-22-2016 16:37:42 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-21-2016 01:04:17 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp1586.jpg

User or Person Being Reported

Screen/User Name: jvt12345615
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp1586.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A2
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

119,12,6,60,114,45,17,176,101,114,26,143,8,182,80,21,11,11,20,11,17,0,
4,14,53,11,9,52,175,61,28,99,140,108,59,111,31,138,110,195,31,90,85,8
2,27,28,37,42,42,20,158,10,136,73,109,41,95,220,42,118,119,90,104,100
,73,135,173,58,99,48,57,51,38,14,29,69,76,87,46,44,56,178,59,50,163,20
,100,59,87,131,117,129,70,86,122,18,53,17,14,114,66,38,25,152,18,86,4
2,110,30,33,15,113,89,85,33,179,101,26,36,155,28,49,34,104,50,24,11,1
34,4,18,0,123,9,6,0,85,48,40,27,86,62,26,36,75

Original URL Where File was Located:

D:\local\Temp\tmp1586.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
Online Services:

FAX: (425) 708-0096 Microsoft Corporation

Attn: Online Services Custodian of Records

One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A2: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12651690



CyberTipline Report 12651697

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-22-2016 16:37:44 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-21-2016 01:27:49 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp1B09.jpg

User or Person Being Reported

Screen/User Name: jvt12345615
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp1B09.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A1
(See Section B for further explanation)



Original Binary Hash of File (PhotoDNA): 108,27,7,255,100,48,61,230,76,48,82,190,38,46,10,240,41,5,0,255,66,0,0,155,24,17,29,90,94,7,25,182,118,40,35,233,28,131,8,143,72,14,0,168,14,5,0,0,143,7,29,6,61,84,6,17,74,89,24,51,61,19,112,16,43,54,37,14,49,153,0,4,57,8,22,35,7,72,6,73,19,81,22,32,56,23,56,34,33,36,16,102,1,105,1,4,3,2,43,9,72,0,81,16,132,6,45,60,127,12,82,28,143,2,57,51,128,0,65,12,60,0,49,54,93,0,135,12,174,8,39,33,208,17,54,19,177,4,32,85,190,0,37,34,107,0

Original URL Where File was Located: D:\local\Temp\tmp1B09.jpg

Additional Information: Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other Online Services:
 FAX: (425) 708-0096 Microsoft Corporation
 Attn: Online Services Custodian of Records
 One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS
 Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT
 Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12651697



CyberTipline Report 12651701

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-22-2016 16:37:45 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-21-2016 01:42:46 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp204D.jpg

User or Person Being Reported

Screen/User Name: jvt12345615
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp204D.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A1
(See Section B for further explanation)



Original Binary Hash of File (PhotoDNA): 32,150,1,113,250,5,0,127,71,0,7,44,21,2,10,11,29,8,8,3,24,0,4,1,26,81,15,52,239,2,8,67,178,0,12,55,29,3,14,0,28,15,13,4,21,7,1,9,19,94,68,21,138,15,29,47,255,13,5,154,62,7,11,20,19,46,8,54,32,35,0,125,37,122,111,30,51,53,46,37,255,40,24,101,140,37,0,108,19,157,13,191,93,42,61,109,41,116,72,71,56,40,128,31,131,74,117,68,100,105,10,231,168,83,70,134,12,6,4,99,6,21,65,208,5,39,86,156,43,21,77,38,69,10,57,3,61,244,10,19,43,7,5,1,14,18

Original URL Where File was Located: D:\local\Temp\tmp204D.jpg

Additional Information: Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other Online Services:
 FAX: (425) 708-0096 Microsoft Corporation
 Attn: Online Services Custodian of Records
 One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12651701



CyberTipline Report 12765571

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-27-2016 16:14:01 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*

Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-26-2016 01:01:29 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp247D.jpg

User or Person Being Reported

Screen/User Name: vtj12315
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp247D.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A1
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

142,39,27,86,140,4,17,30,42,66,15,45,0,141,36,99,18,126,53,60,97,13,57,33,114,80,88,34,142,10,29,136,28,165,12,158,17,130,43,167,33,100,50,107,98,24,22,143,65,40,94,50,42,44,170,118,37,75,152,131,80,64,126,45,48,186,187,55,45,76,68,26,51,15,150,1,31,19,118,6,18,86,150,16,38,166,115,72,54,116,68,119,113,40,177,10,57,53,55,8,29,66,21,47,48,39,31,16,24,176,188,23,94,44,231,14,122,4,166,17,13,83,25,3,69,98,41,30,54,10,44,9,20,34,57,4,28,80,77,46,86,28,32,83

Original URL Where File was Located:

D:\local\Temp\tmp247D.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other Online Services:

FAX: (425) 708-0096 Microsoft Corporation

Attn: Online Services Custodian of Records

One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12765571



CyberTipline Report 12765579

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-27-2016 16:14:03 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*
Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-26-2016 01:02:13 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp2D7C.jpg

User or Person Being Reported

Screen/User Name: vtj12315
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp2D7C.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A1
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

100,29,16,49,217,10,5,158,37,86,5,143,70,28,12,74,6,35,11,20,1,204,1,1
 28,29,45,19,16,238,26,7,127,107,102,47,69,117,38,46,56,10,151,3,125,2
 9,167,10,106,8,62,29,2,109,42,18,62,199,22,36,135,96,149,52,110,25,20
 0,15,146,67,45,35,26,27,127,52,8,35,79,40,12,132,18,13,119,62,93,16,19
 8,49,113,31,77,83,40,56,12,50,142,102,15,41,150,105,15,44,34,13,33,26,
 44,6,36,129,20,68,15,96,73,137,24,92,76,136,32,17,186,87,55,28,69,63,4
 ,44,37,47,5,148,9,62,50,140,26,105,128

Original URL Where File was Located:

D:\local\Temp\tmp2D7C.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
 Online Services:

FAX: (425) 708-0096 Microsoft Corporation
 Attn: Online Services Custodian of Records
 One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A1: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 12766078, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12765579



CyberTipline Report 12766078

Priority Level: E

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 06-27-2016 16:27:18 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief summary of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

Total Uploaded Files: 1

Uploaded File Categorization: *(uploaded files may or may not be categorized)*

Uncategorized: 1

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and makes information submitted to the CyberTipline available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC is not an agent or instrumentality of the government or law enforcement agency and does not act in the capacity of or under the direction or control of a government or law enforcement agency. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.



Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Incident Information	1
Peer to Peer	1
User or Person Being Reported	1
Uploaded File Information	1
Uploaded File Information	1
Section B: Automated Information Added by NCMEC Systems	3
Explanation of Automated Information (in alphabetical order)	3
Further Information on Uploaded Files	3
Geo-Lookup (Reported Person or User)	3
Geo-Lookup (Uploaded Files)	3
Section C: Additional Information Provided by NCMEC	5
NCMEC Note #1	5
NCMEC Note #2	5
Section D: Law Enforcement Contact Information	6
Vermont Office of Attorney General	6



Section A: Reported Information

The following information was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - SBO (Skype)
Microsoft SBO on behalf of CVS4Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 06-26-2016 01:03:05 UTC

Peer to Peer

Peer-to-Peer Client: CVS4Skype
IP_ADDRESS: 24.91.154.58
Peer to Peer Filenames: tmp4DB5.jpg

User or Person Being Reported

Screen/User Name: vtj12315
IP Address: 24.91.154.58
Device ID (CVS4Skype): unknown

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename: tmp4DB5.jpg
Was File Reviewed by Company? Yes
Child Pornography Categorization by ESP: A2
(See Section B for further explanation)

**Original Binary Hash of File (PhotoDNA):**

11,122,186,0,99,31,240,0,86,10,169,1,95,32,190,4,155,18,96,9,9,255,30,
6,35,37,97,100,29,17,142,136,59,60,91,155,68,57,66,219,142,12,13,182,
40,226,74,28,3,81,24,52,39,12,38,74,84,65,127,91,47,84,175,63,185,6,76
,65,120,30,47,27,47,37,125,3,33,39,171,13,134,28,101,3,30,95,120,0,103
,14,99,1,86,24,48,11,43,9,19,44,32,50,23,75,127,14,51,42,37,86,55,9,66,
30,36,12,66,51,13,52,23,48,12,61,38,61,5,126,129,20,11,177,114,39,35,6
4,15,51,56,2,34,48,21,31

Original URL Where File was Located:

D:\local\Temp\tmp4DB5.jpg

Additional Information:

Where to serve legal process in Criminal Matters

Windows Live TM, Windows Live Id (Passport), MSNA, Xbox & Other
Online Services:

FAX: (425) 708-0096 Microsoft Corporation
Attn: Online Services Custodian of Records
One Microsoft Way Redmond, WA 98052-6399

EMERGENCY REQUESTS

Microsoft Online Services will respond to emergency requests outside of normal business hours if the emergency involves the danger of death or physical injury to any person as permitted in 18 U.S.C. A 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorism threats, etc. If you have an emergency request, please call the law enforcement hotline at (425) 722-1299.

NON-U.S. LAW ENFORCEMENT

Microsoft has established local contacts within your country or region to handle legal process related to Microsoft Online Services. If you are not already familiar with your local contact, please e-mail the Global Criminal Compliance team at globalcc@microsoft.com, and you will be directed to the local contact handling requests from your country. All legal process for criminal matters from non-U.S. law enforcement, prosecutors and courts must be direct to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 and not to Microsoft local subsidiary as all Microsoft Online Services customer data is stored in the U.S. Your local contact will be able to educate you as to what local process must be followed in order to obtain online services customer account records from Microsoft.

Source Information:

Type	Value	Event	Date/Time
IP Address	24.91.154.58		
Device ID (CVS4Skype)	unknown		

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.



Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "User or Person Being Reported," NCMEC Systems will geographically resolve the IP address via a publicly-available online search. The results of this lookup are displayed.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A2: 1

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Reported Person or User)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
24.91.154.58	US	VT	Bennington	Albany-Schenectady-Troy	05201		42.8626 / -73.0998	Comcast Cable/ Comcast Cable

Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
------------	---------	--------	------	------------	-------------	-----------	----------	---------



24.91.154.58	US	VT	Bennington	Albany- Schenectady -Troy	05201	42.8626/ 73.0998	-	Comcast Cable/ Comcast Cable
--------------	----	----	------------	---------------------------------	-------	---------------------	---	------------------------------------

This concludes Section B



Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from searches on publicly-available, open-source websites. Any searches conducted by NCMEC staff will be documented and any search results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification	Apparent Child Pornography
NCMEC Date Processed:	06-28-2016 16:02:59 UTC
Made Available to Law Enforcement by NCMEC:	Yes
Associated CyberTipline Reports:	12627584, 12469951, 12765571, 12050739, 12627589, 12765579, 12051516, 12050735, 12050728, 12627552, 12051925, 12415578, 11751259, 12468566, 11751258, 12415511, 12415510, 12651690, 12468560, 12045016, 12527760, 12526159, 12651697, 12469964, 12526157, 12526156, 12469962, 12526155, 12651701, 12415755, 12469960, 12526153, 12526152, 12527752, 12526151, 12526150, 12526149, 11614028

NCMEC Note #1

ECD-NB 06-28-2016 15:49:31 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

NCMEC Note #2

ECD-NB 06-28-2016 16:02:59 UTC

There are multiple reports on this target. Please see CT #11614028 for all analysis.

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.



Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

Vermont Office of Attorney General

Investigator:

Assigned Officer:	Access VPN
Title:	Detective Matthew Raymond
City/State:	Montpelier, VT
Country:	United States
Phone Number:	802-828-5522
Email Address:	matthew.raymond@vermont.gov

Time/Date was made available: 06-28-2016 16:02:59 UTC

This concludes Section D

This concludes CyberTipline Report 12766078

EXHIBIT B

Microsoft Services Agreement

Posted: June 11, 2014; Effective: July 31, 2014

IF YOU LIVE IN THE UNITED STATES, SECTION 10 CONTAINS A BINDING ARBITRATION CLAUSE AND CLASS ACTION WAIVER. IT AFFECTS YOUR RIGHTS ABOUT HOW TO RESOLVE ANY DISPUTE WITH MICROSOFT. PLEASE READ IT.

Thank you for choosing Microsoft! This is an agreement between you and Microsoft Corporation (or based on where you live one of its affiliates) that describes your rights to use the software and services identified in section 1.1. For your convenience, we have phrased some of the terms of this Agreement in a question and answer format. You should read the entire Agreement because all of the terms are important and together create a legal agreement that, once accepted by you, applies to you.

1. Scope of Agreement, acceptance, and changes

1.1 What services are covered by this Agreement? Outlook.com (formerly Hotmail), OneDrive (formerly SkyDrive), Microsoft account, Microsoft Family Safety, Windows Photo Gallery, Windows Movie Maker, Windows Live Mail, Windows Live Writer (these services are collectively referred to as the “Windows Services”); Office.com, Microsoft Office 365 Home Premium, Microsoft Office 365 University, and other Microsoft Office-branded services that link to this Agreement through a supplemental agreement (the “Office Services”); Bing; and MSN are the primary services this Agreement covers. We refer to these services, as well as other software, websites, and services that link to this Agreement collectively as the “Services.” When using the Services, you must abide by these terms (“this Agreement”).

1.2 How do I accept this Agreement? By using or accessing the Services, or by agreeing to these terms where the option is made available to you in the user interface, you agree to abide by this Agreement without modification by you. If you do not agree, you may not use the Services.

1.3 Can Microsoft change this Agreement after I have accepted it? Yes. From time to time, Microsoft may change or amend these terms. If we do, we will notify you, either through the user interface, in an email message, or through other reasonable means. If you use the Services after the date the change becomes effective, you consent to the changed terms. If you do not agree to the changes, you must stop using the Services, cancel any paid Services by following the instructions in section 9.10, and close your Microsoft account. Otherwise, the new terms will apply to you.

1.4 What types of changes can I expect to the Services? We continuously work to improve the Services and may change the Services at any time. We may release the Services or their features in a beta version, which may not work correctly or in the same way the final version may work. From time to time we may stop providing portions of the Services. We may do so for example if it's no longer feasible for us to provide a Service, the technology advances, customer feedback indicates a change is needed, our agreements with third parties no longer permit us to make their material available, or external issues arise that make it imprudent or impractical to continue.

1.5 What age do I have to be to use the Services? By using the Services, you represent that you have either reached the age of “majority” where you live or have valid parent or legal guardian consent to be bound by the terms of this Agreement. If you do not know whether you have reached the age of majority where you live, or do not understand this section, please do not create an account before you have asked your parent or legal guardian for help. If you are the parent or legal guardian of a minor that creates an

account, you accept this Agreement on the minor's behalf and are responsible for all use of the accounts or Services, including purchases, whether the minor's account is now open or created later.

2. Microsoft account

2.1 What is a Microsoft account? Microsoft account is a service that lets you sign in to Microsoft products, websites and services, as well as those of select Microsoft partners. When creating a Microsoft account we ask you to provide certain information, like your name and password, birthdate, certain demographic information, and security information such as an alternate email address or phone number. The email address or user name that you use to create your Microsoft account will be unique to you for as long as your Microsoft account is still active. In the event your Microsoft account is closed either by you or by Microsoft pursuant to the terms of this Agreement, the email address or username may be recycled into our system and assigned to another user. Existing Microsoft account holders may need to provide security information to continue using their Microsoft account. To access and manage your Microsoft account and security information, you can visit (<https://account.live.com/proofs/Manage>). To access the Windows Services and Office Services, you must be logged in with a Microsoft account. **Please review the Privacy Statements (as defined below) to understand how Microsoft collects and uses the information associated with your Microsoft account.** You are responsible for keeping your account information and password confidential and are responsible for all activity that occurs under your Microsoft account. You can use your Microsoft account to gain access to other Microsoft products, websites, or services (like Windows, Xbox Services, and Windows Phone). If you do so, the terms and conditions for those products, websites, or services, including their respective privacy statements, if different from this Agreement, may also apply to your use of those products, websites or services. **You must sign into your Microsoft account periodically, at a minimum every year, to keep services associated with your Microsoft account active, unless provided otherwise in an offer for a paid portion of the Services. If you do not sign in during this period, we will close your account (which means you won't have access to the Windows Services, Office Services, Content stored in your account, and any other product or service that uses Microsoft account). If your Services are cancelled, we will delete information or Content (as defined below) associated with your Microsoft account, or will otherwise disassociate it from you and your Microsoft account, unless the law requires us to keep it.**

2.2 What if I can't access my Microsoft account? If you have forgotten your password or otherwise can't access your Microsoft account, you may recover your Microsoft account by visiting the reset your password webpage (<http://go.microsoft.com/fwlink/?LinkId=238656>). We will do our best to help you recover your Microsoft account, however we cannot guarantee that your Microsoft account will be restored or your Content will be recovered.

2.3 What if I obtained my Microsoft account from someone other than Microsoft? Microsoft does not permit users to transfer their Microsoft accounts, though in some cases, we allow you to obtain your Microsoft account through a third party, like a school, a business, an Internet service provider, or the administrator of a managed domain (<http://www.domains.live.com>). In such cases, that third party may have additional rights over your Microsoft account, like the ability to reset your password, view your account usage or profile data, read or store Content in your account, or suspend or cancel your Microsoft account. In these cases, you are subject to this Agreement and any additional terms of use from that third party, which should be made available to you by such third-party. Microsoft has no responsibility in relation to third parties' additional terms of use. If you are the administrator of a managed domain, you are responsible for all activity that takes place within the accounts on that domain.

3. Content

3.1 Who owns my Content that I put on the Services? You do. Some Services enable you to communicate with others and share or store various types of files, such as photos, documents, music and video. The contents of your communications and your files are your “Content” and, except for material that we license to you that may be incorporated into your own Content (such as clip art), we do not claim ownership of the Content you provide on the Services. Your Content remains your Content, and you are responsible for it.

3.2 Who can access my Content? You have initial control over who may access your Content. However, if you share Content in public areas of the Services, through features that permit public sharing of Content, or in shared areas available to others you’ve chosen, you agree that anyone you have shared Content with may, for free, use, save, reproduce, distribute, display, and transmit that Content in connection with their use of the Services and other Microsoft, or its licensees’, products and services. If you do not want others to have that ability, do not use the Services to share your Content. You represent and warrant that for the duration of this Agreement you have (and will have) all the rights necessary for the Content you upload or share on the Services and that the use of the Content, as contemplated in this section 3.2, won’t violate any law.

3.3 What does Microsoft do with my Content? When you transmit or upload Content to the Services, you are giving Microsoft the worldwide right, without charge, to use Content as necessary: to provide the Services to you, to protect you, and to improve Microsoft products and services. Microsoft uses and protects your Content as outlined in the Windows Services Privacy Statement (<http://go.microsoft.com/fwlink/?LinkId=253457>), Bing Privacy Statement (<http://go.microsoft.com/fwlink/?LinkId=248686>), MSN Privacy Statement (<http://go.microsoft.com/fwlink/?LinkId=248688>), and Office Services Privacy Statement (<http://go.microsoft.com/fwlink/?LinkId=327851>) (collectively the “Privacy Statements”).

3.4 What types of advertising are used by the Services? Some of the Services are supported by advertising. Controls for how Microsoft personalizes advertising are available at <http://choice.live.com> (<http://go.microsoft.com/fwlink/?LinkId=286759>). We do not use what you say in email, chat, video calls or voice mail to target advertising to you. We do not use your documents, photos or other personal files to target advertising to you. Our advertising policies are covered in detail in the Privacy Statements.

3.5 Does Microsoft have voice enabled services? Yes. If you use a Service that is voice enabled, you consent to Microsoft recording and collecting your voice input for use by Microsoft to improve the quality and accuracy of voice enabled services and as further described in the Privacy Statements.

3.6 What type of Content or actions are not permitted? In order to protect our customers and the Services, we have established this Code of Conduct governing the use of the Services. Content or actions that violate this Agreement are not permitted.

- i. Do not use the Services to do anything illegal.
- ii. Do not engage in any activity that exploits, harms, or threatens to harm children.
- iii. Do not send spam or use your account to help others send spam. Spam is unsolicited bulk email, postings or instant messages.
- iv. Do not publicly display inappropriate images (e.g. nudity, bestiality, pornography).
- v. Do not engage in activity that is false or misleading (e.g. attempts to ask for money under false pretenses, impersonating someone else).
- vi. Do not engage in activity that is harmful to the Services or others (e.g. viruses, stalking, hate speech, advocating violence against others).
- vii. Do not infringe upon the rights of others (e.g. unauthorized sharing of copyrighted music, resale or other distribution of Bing maps, photographs and other Content).

viii. Do not engage in activity that violates the privacy of others.

In many cases Microsoft is alerted to violations of the Code of Conduct through customer complaints, but we also deploy automated technologies to detect child pornography or abusive behavior that might harm the system, our customers or others. When investigating these matters, Microsoft or its agents will review Content in order to resolve the issue. This is in addition to the uses we describe in this Agreement and the Privacy Statements.

3.7 Can Microsoft remove my Content from the Services? Yes. Microsoft will remove, limit distribution of, or disable access to your Content if we determine it's in violation of this Agreement, we receive a complaint from another user, we receive a notice of intellectual property infringement, or other legal instruction for removal. We may also block delivery of a communication (like email or instant message) to or from the Services as part of our effort to protect the Services or our customers, or otherwise enforce the terms of this Agreement.

4. Services cancellation

4.1 What happens if I do not abide by this Agreement? If you violate this Agreement, there are a range of actions we may take including removing your Content from the Services, suspending or cancelling your access to the Services, disabling or terminating your Microsoft account (which means you may no longer have access to those Microsoft products, services, or Content connected to your Microsoft account), and/or referring such activity to appropriate authorities. Content that is deleted may be irretrievable.

4.2 Are there other ways I could lose access to the Services? Yes. Failing to sign into your Microsoft account (whether through Outlook.com, OneDrive, or any other service that uses Microsoft account) at least once every year (see section 2.1) means that you won't be able to access the Services and you will lose your Content (unless provided otherwise in an offer for paid Services). Additionally, Microsoft may stop providing portions of the Services, in accordance with section 1.4 above. If you sign up for a paid portion of the Services and fail to make an on-time payment, we may suspend or cancel that Service (see section 9.1 for more details).

4.3 How can I terminate the Services? You may terminate the Services associated with your Microsoft account at any time and for any reason by going to <https://account.live.com/closeaccount.aspx>. To cancel a paid portion of the Services, see section 9.10. If you are canceling your Services, the quickest means of eliminating your Content on the Services is to manually remove it from the various components of the Services (for example, manually delete your email). However, please note that while Content you have deleted or that is associated with a closed account may not be accessible to you, it may still remain on our systems for a period of time. Please see the Privacy Statements for more information about Microsoft's retention practices.

4.4 What happens if my Services are canceled or terminated? If your Services are canceled or terminated (whether by you or us), your right to use the Services stops immediately and your license to use the software related to the Services ends. You must then uninstall that software, or, alternatively, we may disable it. If your Microsoft account is closed (whether by you or us), your right to use your Microsoft account stops immediately. **If any your Services are canceled or terminated, or if your Microsoft account is closed, we will delete information or Content associated with your Microsoft account or will otherwise disassociate it from you and your Microsoft account. We are under no obligation to return Content to you.**

5. Privacy

Your privacy is important to us. We describe how we use and protect your Content and any information we collect from you in the Privacy Statements. They are important so please read them carefully. This Agreement incorporates the Privacy Statements by reference. By using the Services or agreeing to these terms, you consent to Microsoft's collection, use and disclosure of your Content and information as described in the Privacy Statements.

6. Services disruptions and backup

We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft isn't liable for any disruption or loss you may suffer as a result. You should regularly backup the Content that you store on the Services. Having a regular backup plan and following it can help you prevent loss of your Content. We make an effort to provide detailed service status at <http://status.live.com>.

7. Software and related Services

7.1 What terms govern the software that is part of the Services? Unless accompanied by a separate license agreement, any software provided by us to you as part of the Services is subject to the terms of this Agreement. The software is licensed, not sold, and Microsoft reserves all rights to the software not expressly granted by Microsoft, whether by implication, estoppel, or otherwise. If this Agreement governs the website you are viewing, any third party scripts or code, linked to or referenced from this website, are licensed to you by the third parties that own such code, not by Microsoft.

7.2 How can I use the software that is provided as part of the Services? We grant you the right to install and use one copy of the software per device on a worldwide basis for use by only one person at a time as part of your use of the Services, but only if you comply with all other terms in this Agreement.

7.3 Are there things I can't do with the software or Services? Yes. In addition to the other restrictions in this Agreement, you may not circumvent or bypass any technological protection measures in or relating to the software or Services or disassemble, decompile, or reverse engineer any software or other aspect of the Services that is included in or accessible through the Services, except and only to the extent that the applicable copyright law expressly permits doing so; separate components of the software or Services for use on different devices; publish, copy, rent, lease, or lend the software or the Services; or transfer the software, any software licenses, or any rights to access or use the Services. You may not use the Services in any unauthorized way that could interfere with anyone else's use of them or gain access to any service, data, account, or network. You may not enable access to the Services by unauthorized third-party applications.

7.4 How is the software updated? We may automatically check your version of the software. We may also automatically download updates to the software from time to time. You agree to accept such updates subject to these terms unless other terms accompany the updates. If so, those other terms apply. Microsoft isn't obligated to make any updates available and doesn't guarantee that we will support the version of the system for which you licensed the software.

8. Additional terms for Office Services, MSN, and Bing

8.1 Office Services media elements and templates. If you use Office Services, you may have access to media images, clip art, animations, sounds, music, video clips, templates, and other forms of material ("media elements") provided with the software available on Office.com or as part of services associated with the software. Microsoft grants you a license to copy, distribute, perform and display media elements included with the Office Services in projects and documents, except that you may not (i) sell, license, or distribute

copies of the media elements by themselves or as a product if the primary value of the product is the media elements; (ii) grant your customers rights to further license or distribute the media elements; (iii) license or distribute for commercial purposes media elements that include the representation of identifiable individuals, governments, logos, trademarks, or emblems or use these types of images in ways that could imply an endorsement or association with your product, entity or activity; or (iv) create obscene or scandalous works using the media elements. Other media elements, which are accessible on other websites through some Office Services, are governed by the terms on those websites.

8.2 Bing and MSN Materials. The articles, photos, videos, third-party material and embeddable video player available on Bing and MSN are for your non-commercial, personal use only and, unless otherwise stated elsewhere in this Agreement or expressly permitted by Microsoft, may not be downloaded, copied, published, rented, leased, lent, or redistributed without authorization from the rights holders, except and only to the extent that the applicable copyright law expressly permits doing so. This material is licensed, not sold, and Microsoft or other rights holders reserve all rights to the material not expressly granted by Microsoft under the license terms, whether by implication, estoppel, or otherwise. Third parties may choose to make additional material or services available for sale or license within Bing or MSN. Microsoft isn't responsible for such material or services. You may not use the embeddable video player on any website whose purpose is primarily for the display of advertising or collection of subscription revenues or is in direct competition with Bing or MSN unless you first get our express, written consent. You agree that your use of the embeddable video player may result in additional third-party costs, fees, and royalties, including applicable public performance royalties in your country or region.

8.3 Bing Maps Bird's Eye imagery. For Bing Maps, you may not use Bird's eye imagery of the United States, Canada, Mexico, New Zealand, Australia or Japan for governmental use without our separate written approval.

9. If you pay Microsoft, the following terms apply to you

9.1 Charges. If there is a charge associated with a portion of the Services, you agree to pay that charge. The price stated for the Service excludes all applicable taxes and currency exchange settlements, unless stated otherwise. You are solely responsible for paying such taxes or other charges. **We may suspend or cancel the Services if we do not receive an on-time, full payment from you.** Suspension or cancellation of the Services for non-payment could result in a loss of access to and use of your account and its Content.

9.2 Your billing account. To pay the charges for a Service, you will be asked to provide a payment method at the time you sign up for that Service. You can access and change your billing account information and payment method on the Billing and Account Management website (<https://commerce.microsoft.com>). Additionally, you agree to permit Microsoft to use any updated account information regarding your payment method provided by your issuing bank or the applicable payment network. You agree to keep your billing account information current at all times. Changes made to your billing account won't affect charges we submit to your billing account before we could reasonably act on your changes to your billing account.

9.3 Billing. By providing Microsoft with a payment method, you (i) represent that you are authorized to use the payment method that you provided and that any payment information you provide is true and accurate; (ii) authorize Microsoft to charge you for the Services using your payment method; and (iii) authorize Microsoft to charge you for any paid feature of the Services that you choose to sign up for or use while this Agreement is in force. We may bill you (a) in advance; (b) at the time of purchase; (c) shortly after purchase; or (d) on a recurring basis for subscription Services. Also, we may charge you up to the amount you've approved, and we'll notify you in advance of any change in the amount to be charged for recurring

subscription Services. We may bill you at the same time for more than one of your prior billing periods for amounts that haven't previously been processed.

9.4 Automatic renewal. Provided that automatic renewals are allowed in your country, province, or state, we will inform you by email before automatically renewing your Services. Once we have informed you that the Services will be automatically renewed, we may automatically renew your Services and charge you the then current price for the renewal term. We will also remind you that we will bill your chosen payment method for the Services renewal, whether it was on file on the renewal date or provided later. We will also provide you with instructions on how you may cancel the Services. You must cancel the Services before the renewal date to avoid being billed for the renewal.

9.5 Online statement and errors. We will provide you with an online billing statement on the Billing and Account Management website (<https://commerce.microsoft.com>), where you can view and print your statement. This is the only billing statement that we provide. **It's your responsibility to print or save a copy of each online statement and retain such copy for your records.** If we make an error on your bill, you must tell us within 120 days after the error first appears on your bill. We will then promptly investigate the charge. If you do not tell us within that time, you release us from all liability and claims of loss resulting from the error and we won't be required to correct the error or provide a refund. If Microsoft has identified a billing error, we will correct that error within 90 days.

9.6 Cooling off period. When you request a Service from us, you agree that we may begin to provide the Services immediately. You won't be entitled to a cancellation or "cooling off" period, except if the law requires a cooling off period. You may cancel paid Services as provided in section 9.10.

9.7 Trial-period offers. If you are taking part in any trial period offer, you must cancel the Services by the end of the trial period to avoid incurring new charges, unless we notify you otherwise. If you do not cancel your Services at the end of the trial period, we may charge you for the Services.

9.8 Price changes. We may change the price of the Services at any time and will notify you by email at least 15 days before the price change. If you do not agree to the price change, you must cancel and stop using the Services before the price change takes effect. If there is a fixed term and price for your Service offer, that price will remain in force for the term.

9.9 Refund policies. Unless otherwise provided by law or by a particular Service offer, all purchases are final and non-refundable.

9.10 Canceling the Services. You may cancel the Services at any time, with or without cause. Information and direction on how to cancel your Services is provided on the Billing and Account Management website (<https://commerce.microsoft.com>). You should refer back to the offer describing the Services as (i) you may not receive a refund at the time of cancellation; (ii) you may be obligated to pay cancellation charges; (iii) you may be obligated to pay all charges made to your billing account for the Services before the date of cancellation; or (iv) you may lose access to and use of your account when you cancel the Services. If you cancel, your Services will end at the end of your current Service period or, if we bill your account on a periodic basis, at the end of the period in which you canceled.

9.11 Late payments. You must pay for all reasonable costs we incur to collect any past due amounts. These include reasonable attorneys' fees and other legal fees and costs.

9.12 Payments to you. If we owe you a payment, then you agree to timely and accurately provide us with any information we need to get that payment to you. You are responsible for any taxes and charges you may

incur as a result of this payment to you. You must also comply with any other conditions we place on your right to any payment. **If you receive a payment in error, we may reverse or require return of the payment. You agree to cooperate with us in our efforts to do this. We may also reduce the payment to you without notice to adjust for any previous overpayment.**

9.13 Internet access Services and charges. If the Services do not include Internet access, you are responsible for paying the fees charged by your Internet access or Wi-Fi providers. Those fees are in addition to the fees you pay us for the Services. If you access the Services through wireless devices (for example, mobile phones, tablets), your wireless carrier may charge fees for alerts, web browsing, messaging, and other services that require the use of airtime and wireless data services. Check with your carrier to verify whether there are any such fees that may apply to you. You are solely responsible for any costs you incur to access the Services through any wireless or other communication service.

The rest of this section 9.13 applies only if your Services include Internet access. Internet access is not available outside the United States. If you use a dial-up modem, you may incur toll, roaming, or other access charges, depending on the number you call and from where you call. You should check with your local telephone company first to determine if the number you plan to use will incur such charges. Even if we suggest a phone number for you to call, you may still incur charges, depending on your local provider, calling location, and phone plan. We won't reimburse you for such charges.

10. BINDING ARBITRATION AND CLASS ACTION WAIVER IF YOU LIVE IN THE UNITED STATES

This section applies to any dispute **EXCEPT DISPUTES RELATING TO THE ENFORCEMENT OR VALIDITY OF YOUR, YOUR LICENSORS', MICROSOFT'S, OR MICROSOFT'S LICENSORS' INTELLECTUAL PROPERTY RIGHTS.** The term "dispute" means any dispute, action, or other controversy between you and Microsoft concerning the Services (including their price) or this Agreement, whether in contract, warranty, tort, statute, regulation, ordinance, or any other legal or equitable basis. "Dispute" will be given the broadest possible meaning allowable under law.

10.1 Notice of Dispute. In the event of a dispute, you or Microsoft must give the other a Notice of Dispute, which is a written statement that sets forth the name, address and contact information of the party giving it, the facts giving rise to the dispute, and the relief requested. You must send any Notice of Dispute by U.S. Mail to **Microsoft Corporation, ATTN: LCA ARBITRATION, One Microsoft Way, Redmond, WA 98052-6399, U.S.A.** A form is available on the Legal and Corporate Affairs (LCA) website (<http://go.microsoft.com/fwlink/?LinkId=245499>). Microsoft will send any Notice of Dispute to you by U.S. Mail to your address if we have it, or otherwise to your email address. You and Microsoft will attempt to resolve any dispute through informal negotiation within 60 days from the date the Notice of Dispute is sent. After 60 days, you or Microsoft may commence arbitration.

10.2 Small claims court. You may also litigate any dispute in small claims court in your county of residence or King County, Washington, U.S.A. if the dispute meets all requirements to be heard in the small claims court. You may litigate in small claims court whether or not you negotiated informally first.

10.3 Binding arbitration. If you and Microsoft do not resolve any dispute by informal negotiation or in small claims court, any other effort to resolve the dispute will be conducted exclusively by individual binding arbitration governed by the Federal Arbitration Act ("FAA"). Class arbitrations are not permitted. **You are giving up the right to litigate disputes in court before a judge or jury (or participate in court as a party or class member).** Instead, all disputes will be resolved before a neutral arbitrator, whose decision will be final except for a limited right of appeal under the FAA. Any court with jurisdiction over the parties may enforce the arbitrator's award.

10.4 Class action waiver. Any proceedings to resolve or litigate any dispute in any forum will be conducted solely on an individual basis. Neither you nor Microsoft will seek to have any dispute heard as a class action, private attorney general action, or in any other proceeding in which either party acts or proposes to act in a representative capacity. No arbitration or other proceeding will be combined with another without the prior written consent of all parties to all affected arbitrations or proceedings.

10.5 Arbitration procedure. Any arbitration will be conducted by the American Arbitration Association (the “AAA”) under its Commercial Arbitration Rules. If you are an individual and use the Services for personal or household use, or if the value of the dispute is \$75,000 or less whether or not you are an individual or how you use the Services, its Supplementary Procedures for Consumer-Related Disputes will also apply. For more information, see www.adr.org or call 1-800-778-7879. To commence arbitration, submit the form available on the Legal and Corporate Affairs (LCA) website (<http://go.microsoft.com/fwlink/?LinkId=245497>) to the AAA. You agree to commence arbitration only in your county of residence or in King County, Washington, U.S.A. Microsoft agrees to commence arbitration only in your county of residence. You may request a telephonic or in-person hearing by following the AAA rules. In a dispute involving \$10,000 or less, any hearing will be telephonic unless the arbitrator finds good cause to hold an in-person hearing instead. The arbitrator may award the same damages to you individually as a court could. The arbitrator may award declaratory or injunctive relief only to you individually, and only to the extent required to satisfy your individual claim.

10.6 Arbitration fees and payments.

10.6.1 Disputes involving \$75,000 or less. Microsoft will promptly reimburse your filing fees and pay the AAA’s and arbitrator’s fees and expenses. If you reject Microsoft’s last written settlement offer made before the arbitrator was appointed (“Microsoft’s last written offer”), your dispute goes all the way to an arbitrator’s decision (called an “award”), and the arbitrator awards you more than Microsoft’s last written offer, Microsoft will: (i) pay the greater of the award or \$1,000; (ii) pay twice your reasonable attorney’s fees, if any; and (iii) reimburse any expenses (including expert witness fees and costs) that your attorney reasonably accrues for investigating, preparing, and pursuing your claim in arbitration. The arbitrator will determine the amount of fees, costs, and expenses unless you and Microsoft agree on them.

10.6.2 Disputes involving more than \$75,000. The AAA rules will govern payment of filing fees and the AAA’s and arbitrator’s fees and expenses.

10.6.3 Disputes involving any amount. In any arbitration you commence, Microsoft will seek its AAA or arbitrator’s fees and expenses, or your filing fees if reimbursed, only if the arbitrator finds the arbitration frivolous or brought for an improper purpose. In any arbitration Microsoft commences, Microsoft will pay all filing, AAA, and arbitrator’s fees and expenses. Microsoft won’t seek its attorney’s fees or expenses from you in any arbitration. Fees and expenses are not counted in determining how much a dispute involves.

10.7 Conflict with AAA rules. This Agreement governs to the extent it conflicts with the AAA’s Commercial Arbitration Rules and Supplementary Procedures for Consumer-Related Disputes.

10.8 Claims or disputes must be filed within one year. To the extent permitted by law, any claim or dispute to which section 10 applies must be filed within one year in small claims court (section 10.2) or in arbitration (section 10.3). The one-year period begins when the claim or Notice of Dispute first could be filed. If such a claim or dispute isn’t filed within one year, it’s permanently barred.

10.9 Rejecting future arbitration changes. You may reject any change Microsoft makes to section 10 (other than address changes) by sending us notice within 30 days of the change by U.S. Mail to the address in section 10.1. If you do, the most recent version of section 10 before the change you rejected will apply.

10.10 Severability. If the class action waiver in section 10.4 is found to be illegal or unenforceable as to all or some parts of a dispute, then section 10 won't apply to those parts. Instead, those parts will be severed and proceed in a court of law, with the remaining parts proceeding in arbitration. If any other provision of section 10 is found to be illegal or unenforceable, that provision will be severed with the remainder of section 10 remaining in full force and effect.

11. NO WARRANTIES

MICROSOFT, AND OUR AFFILIATES, RESELLERS, DISTRIBUTORS, AND VENDORS, MAKE NO WARRANTIES, EXPRESS OR IMPLIED, GUARANTEES OR CONDITIONS WITH RESPECT TO YOUR USE OF THE SERVICES. YOU UNDERSTAND THAT USE OF THE SERVICES IS AT YOUR OWN RISK AND THAT WE PROVIDE THE SERVICES ON AN "AS IS" BASIS "WITH ALL FAULTS" AND "AS AVAILABLE." MICROSOFT DOESN'T GUARANTEE THE ACCURACY OR TIMELINESS OF INFORMATION AVAILABLE FROM THE SERVICES. TO THE EXTENT PERMITTED UNDER YOUR LOCAL LAW, WE EXCLUDE ANY IMPLIED WARRANTIES, INCLUDING FOR MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, WORKMANLIKE EFFORT, AND NON-INFRINGEMENT. YOU MAY HAVE CERTAIN RIGHTS UNDER YOUR LOCAL LAW. NOTHING IN THIS AGREEMENT IS INTENDED TO AFFECT THOSE RIGHTS, IF THEY ARE APPLICABLE.

YOU ACKNOWLEDGE THAT COMPUTER AND TELECOMMUNICATIONS SYSTEMS ARE NOT FAULT-FREE AND OCCASIONAL PERIODS OF DOWNTIME OCCUR. WE DO NOT GUARANTEE THE SERVICES WILL BE UNINTERRUPTED, TIMELY, SECURE, OR ERROR-FREE OR THAT CONTENT LOSS WON'T OCCUR.

12. Limitation of Liability

If Microsoft breaches this Agreement, you agree that your exclusive remedy is to recover, from Microsoft or any affiliates, resellers, distributors, and vendors, direct damages up to an amount equal to your Services fee for one month (or up to USD\$10.00 if the Services are free). **YOU CAN'T RECOVER ANY OTHER DAMAGES OR LOSSES, INCLUDING, WITHOUT LIMITATION, DIRECT, CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT, INCIDENTAL, OR PUNITIVE.** These limitations and exclusions apply if this remedy doesn't fully compensate you for any losses or fails of its essential purpose or if we knew or should have known about the possibility of the damages. To the maximum extent permitted by law, these limitations and exclusions apply to anything related to this Agreement such as loss of Content; any virus affecting your use of the Services; delays or failures in starting or completing transmissions or transactions; claims for breach of contract, warranty, guarantee, or condition; strict liability, negligence, misrepresentation, omission, trespass, or other tort; violation of statute or regulation; or unjust enrichment. **Some or all of these limitations or exclusions may not apply to you if your state, province, or country doesn't allow the exclusion or limitation of incidental, consequential, or other damages.**

13. Microsoft contracting entity, court of venue, and applicable law – United States

If you live in (or, if you are a business, you are headquartered in) the United States, you are contracting with Microsoft Corporation, One Microsoft Way, Redmond, WA 98052, U.S.A. The laws of the state where you live govern the interpretation of this Agreement, claims for breach of it, and all other claims (including consumer protection, unfair competition, and tort claims), regardless of conflict of law principles, except that the FAA governs all provisions relating to arbitration. You and we irrevocably consent to the exclusive jurisdiction and

venue of the state or federal courts in King County, Washington, for all disputes arising out of or relating to this Agreement or the Services that are heard in court (not arbitration and not small claims court).

14. Third-party websites

You may be able to access third-party websites or services via the Services. Microsoft isn't responsible for third-party websites, services, or material available through those third-party services. You are solely responsible for your dealings with third parties (including advertisers). Your use of third-party websites or services may be subject to that third party's terms and conditions.

15. Digital Rights Management

If you access material protected with digital rights management (DRM), the DRM software may automatically request media usage rights from a rights server online and download and install DRM updates so that you can play the material.

16. Microsoft .NET Framework software

The software may contain Microsoft .NET Framework software. This software is part of Windows. The license terms for Windows apply to your use of the .NET Framework software.

17. Survival

This section, and sections 5, 9 (for amounts incurred before the end of this Agreement), 10, 11, 12, 13, 20, and those that by their terms apply after it ends will survive any termination or cancellation of this Agreement.

18. Assignment and transfer

We may assign this Agreement, in whole or in part, at any time without notice to you. You may not assign this Agreement or transfer any rights to use the Services.

19. Notices

You consent to Microsoft providing you notifications about the Services or information the law requires us to provide via email to the address that you specified when you signed up for the Services. Notices emailed to you will be deemed given and received when the email is sent. If you do not consent to receive notices electronically, you must stop using the Services. You may notify Microsoft as stated in customer support for the Services.

20. Contract interpretation

This is the entire Agreement between you and Microsoft for your use of the Services. It supersedes any prior agreements between you and Microsoft regarding your use of the Services. All parts of this Agreement apply to the maximum extent permitted by relevant law. If a court or arbitrator holds that we can't enforce a part of this Agreement as written, we may replace those terms with similar terms to the extent enforceable under the relevant law, but the rest of this Agreement won't change. Section 10.10 says what happens if parts of section 10 (arbitration and class action waiver) are found to be illegal or unenforceable. Section 10.10 prevails over this section if inconsistent with it.

21. No third-party beneficiaries

This Agreement is solely for your and our benefit. It isn't for the benefit of any other person, except for Microsoft's successors and assigns.

22. Font components

You may use the fonts to display and print material only while using the Services. You may not circumvent any embedding restrictions in the fonts.

23. Support

Customer support for the Windows Services is available via Microsoft Answers (<http://answers.microsoft.com>) and the Windows website (<http://windows.microsoft.com>). Customer support for MSN Internet Access is available at MSN Support (<https://support.msn.com>). Customer email support for Bing and Bing clients is available at Bing Support (<https://support.discoverbing.com>). Limited customer support for Office 365 Home Premium and Office 365 University is available at office.com/support (help/how to) and at support.microsoft.com/ph/13615 (technical support).

24. Export restrictions

Microsoft's free software and services are subject to United States and other jurisdictions' export and technology laws and you agree to comply with all such applicable laws and regulations that apply to the software and/or services. United States government permission is required to transfer these free software and services to governments of any embargoed country or certain prohibited parties. Please see the U.S. Department of Treasury website (<http://go.microsoft.com/fwlink/?LinkId=243206>) for more information. Additionally, paid services are subject to United States export laws and regulations with which you must comply. These laws include restrictions on destinations, end users, and end use. For additional information, see Exporting Microsoft Products website (<http://www.microsoft.com/exporting>).

NOTICES

Notices and procedure for making claims of intellectual property infringement. Microsoft respects the intellectual property rights of third parties. If you wish to send a notice of intellectual property infringement, including claims of copyright infringement, please use our procedures for submitting [Notices of Infringement](https://www.microsoft.com/info/cpyrtInfrg.aspx) (<https://www.microsoft.com/info/cpyrtInfrg.aspx>). **ALL INQUIRIES NOT RELEVANT TO THIS PROCEDURE WILL NOT RECEIVE A RESPONSE.**

Microsoft uses the process set out in Title 17, United States Code, Section 512(c)(2) to respond to notices of copyright infringement. In appropriate circumstances, Microsoft may also disable or terminate accounts of users of Microsoft services who may be repeat infringers.

Notices and procedures regarding intellectual property concerns in advertising. Please review our Intellectual Property Guidelines (<http://go.microsoft.com/fwlink/?LinkId=243207>) regarding intellectual property concerns on our advertising network.

Copyright and trademark notices. All portions of the Services are Copyright © 2013 Microsoft Corporation and/or its suppliers, One Microsoft Way, Redmond, WA 98052, U.S.A. All rights reserved. We or our suppliers own the title, copyright, and other intellectual property rights in the Services and its content. Microsoft and the names, logos, and icons of all Microsoft products, software, and services may be either [trademarks or](#)

registered trademarks of Microsoft in the United States and/or other countries. The names of actual companies and products may be the trademarks of their respective owners. Any rights not expressly granted in this Agreement are reserved. Certain software used in certain Microsoft website servers is based in part on the work of the Independent JPEG Group. Copyright © 1991-1996 Thomas G. Lane. All rights reserved. "gnuplot" software used in certain Microsoft website servers is copyright © 1986-1993 Thomas Williams, Colin Kelley. All rights reserved.

Stock quotes and index data (including index values). © 2013 Morningstar, Inc. All Rights Reserved. The information contained herein: (1) is proprietary to Morningstar and/or its content providers; (2) may not be copied or distributed; and (3) is not warranted to be accurate, complete or timely. Neither Morningstar nor its content providers are responsible for any damages or losses arising from any use of this information. Past performance is no guarantee of future results.

You may not use any of the Dow Jones IndexesSM, index data, or the Dow Jones marks in connection with the issuance, creation, sponsorship, trading, marketing, or promotion of any financial instruments or investment products (for example, derivatives, structured products, investment funds, exchange-traded funds, investment portfolios, etc., where the price, return and/or performance of the instrument or investment product is based on, related to, or intended to track any of the Indexes or a proxy for any of the Indexes) without a separate written agreement with Dow Jones.

Financial notice. Microsoft isn't a broker/dealer or registered investment advisor under United States federal securities law or securities laws of other jurisdictions and doesn't advise individuals as to the advisability of investing in, purchasing, or selling securities or other financial products or services. Nothing contained in the Services is an offer or solicitation to buy or sell any security. Neither Microsoft nor its licensors of stock quotes or index data endorse or recommend any particular financial products or services. Nothing in the Services is intended to be professional advice, including but not limited to, investment or tax advice.

Notice about the H.264/AVC, MPEG-4 Visual, and VC-1 Video Standards. The software may include H.264/AVC, MPEG-4 Visual and/or VC-1 codec technology that may be licensed by MPEG LA, L.L.C. This technology is a format for data compression of video information. MPEG LA, L.L.C. requires this notice:

THIS PRODUCT IS LICENSED UNDER THE H.264/AVC, MPEG-4 VISUAL, AND THE VC-1 PATENT PORTFOLIO LICENSES FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER TO (A) ENCODE VIDEO IN COMPLIANCE WITH THE STANDARDS ("VIDEO STANDARDS") AND/OR (B) DECODE H.264/AVC, MPEG-4 VISUAL, AND VC-1 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE SUCH VIDEO. NONE OF THE LICENSES EXTEND TO ANY OTHER PRODUCT REGARDLESS OF WHETHER SUCH PRODUCT IS INCLUDED WITH THIS SOFTWARE IN A SINGLE ARTICLE. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE THE MPEG LA WEBSITE (<http://www.mpegla.com>).

For clarification purposes only, this notice does not limit or inhibit the use of the software provided under this Agreement for normal business uses that are personal to that business which do not include (i) redistribution of the software to third parties, or (ii) creation of material with the VIDEO STANDARDS compliant technologies for distribution to third parties.



Microsoft Services Agreement

FAQ Microsoft Services Agreement Microsoft Privacy Statement

Published: **June 4, 2015**

Effective: **August 1, 2015**



Microsoft Services Agreement

IF YOU LIVE IN (OR YOUR PRINCIPAL PLACE OF BUSINESS IS IN) THE UNITED STATES, PLEASE READ THE BINDING ARBITRATION CLAUSE AND CLASS ACTION WAIVER IN SECTION 15. IT AFFECTS HOW DISPUTES ARE RESOLVED.

These terms ("**Terms**") cover the use of those Microsoft's consumer products, websites, and services listed [here](#) (the "**Services**"). Many of these products previously had separate terms that were called different names, such as "Xbox Live Terms of Use" or "Skype Terms of Use," and these Terms replace those separate terms. You accept these Terms by creating a Microsoft account or Skype account, through your use of the Services, or by continuing to use the Services after being notified of a change to these Terms.

Your Privacy

Your Content

Code of Conduct

Using the Services & Support

Using Third-Party Apps and Services

Service Availability

Updates to the Services or Software, and Changes to These Terms

Software License

Payment Terms

Contracting entity, choice of law, jurisdiction

Your Privacy

1. **Your Privacy.** Your privacy is important to us. Please read the [Microsoft Privacy Statement](#), the [Microsoft Health Privacy Statement](#), and the [HealthVault Privacy Statement](#) (collectively "**Privacy Statements**") as they describe the types of data we collect from you and your devices ("**Data**") and how we use your Data. The Privacy Statements also describe how Microsoft uses your content, which is your communications with others; postings or feedback submitted by you to Microsoft via the Services; and the files, photos, documents, audio, digital works, and videos that you upload, store or share through the Services ("**Your Content**"). By using the Services or agreeing to these Terms, you consent to Microsoft's collection, use and disclosure of Your Content and Data as described in the Privacy Statements.

Your Content

2. **Your Content.** Many of our Services allow you to store or share Your Content or receive material from others. We don't claim ownership of Your Content. Your Content remains Your Content and you are responsible for it.

a. When you share Your Content with other people, you understand that they may be able to, on a worldwide basis, use, save, record, reproduce, transmit, display (and on HealthVault delete) Your Content without compensating you. If you do not want others to have that ability, do not use the Services to share Your Content. You represent and warrant that for the duration of these Terms, you have (and will

Warranties

Limitation of Liability

Service-Specific
TermsXbox Live and
Microsoft Studios
Games and
Applications

Store

Microsoft Family

Skype

Bing and MSN

Bing Rewards

Cortana

Outlook.com

Office-based
Services

HealthVault

Binding Arbitration
and Class Action
Waiver

Miscellaneous

NOTICES

STANDARD
APPLICATION
LICENSE TERMS

Covered Services

have) all the rights necessary for Your Content that is uploaded, stored or shared on or through the Services and that the collection, use, and retention of Your Content will not violate any law or rights of others. Microsoft cannot be held responsible for Your Content or the material others upload, store or share using the Services.

b. To the extent necessary to provide the Services to you and others, to protect you and the Services, and to improve Microsoft products and services, you grant to Microsoft a worldwide and royalty-free intellectual property license to use Your Content, for example, to make copies of, retain, transmit, reformat, display, and distribute via communication tools Your Content on the Services. If you publish Your Content in areas of the Service where it is available broadly online without restrictions, Your Content may appear in demonstrations or materials that promote the Service. Controls for how Microsoft personalizes advertising are available on the [Security & privacy page](#) of the Microsoft account management website. We do not use what you say in email, chat, video calls or voice mail, or your documents, photos or other personal files to target advertising to you. Our advertising policies are covered in detail in the Privacy Statements.

[↑Top of page](#)

Code of Conduct

3. Code of Conduct.

a. By agreeing to these Terms, you're agreeing that, when using the Services, you will follow these rules:

- i. Don't do anything illegal.
- ii. Don't engage in any activity that exploits, harms, or threatens to harm children.
- iii. Don't send spam. Spam is unwanted or unsolicited bulk email, postings, contact requests, SMS (text messages), or instant messages.
- iv. Don't publicly display or use the Services to share inappropriate Content or material (involving, for example, nudity, bestiality, pornography, graphic violence, or criminal activity).
- v. Don't engage in activity that is false or misleading (e.g., asking for money under false pretenses, impersonating someone else, manipulating the Services to increase play count, or affect rankings, ratings, or comments).
- vi. Don't circumvent any restrictions on access to or availability of the Services.
- vii. Don't engage in activity that is harmful to you, the Services, or others (e.g., transmitting viruses, stalking, communicating hate speech, or advocating violence against others).
- viii. Don't infringe upon the rights of others (e.g., unauthorized sharing of copyrighted music or other copyrighted material, resale or other distribution of Bing maps, or photographs).
- ix. Don't engage in activity that violates the privacy of others.
- x. Don't help others break these rules.

b. **Enforcement.** If you violate these Terms, we may stop providing Services to you or we may close your Microsoft account or Skype account. We may also block delivery of a communication (like email or instant message) to or from the Services in an effort to enforce these Terms or we may remove or refuse to publish Your

Content for any reason. When investigating alleged violations of these Terms, Microsoft reserves the right to review Your Content in order to resolve the issue. However, we cannot monitor the entire Services and make no attempt to do so.

[↑Top of page](#)

Using the Services & Support

4. Using the Services & Support.

a. **Microsoft account or Skype account.** You'll need a Microsoft account to access many of the Services. Your Microsoft account lets you sign in to products, websites and services provided by Microsoft and some Microsoft partners. To access Skype on certain platforms, you have the option of using a Skype account or a Microsoft account.

i. **Creating an Account.** You can create a Microsoft account or a Skype account by signing up online. You agree not to use any false, inaccurate or misleading information when signing up for your Microsoft account or Skype account. In some cases, a third party, like your Internet service provider, may have assigned a Microsoft account to you. If you received your Microsoft account from a third party, the third party may have additional rights over your account, like the ability to access or delete your Microsoft account. Please review any additional terms the third party provided you, as Microsoft has no responsibility regarding these additional terms. If you create a Microsoft account on behalf of an entity, such as your business or employer, you represent that you have the legal authority to bind that entity to these Terms. You cannot transfer your Microsoft account or Skype account to another user or entity. To protect your account, keep your account details and password confidential. You are responsible for all activity that occurs under your Microsoft account or Skype account.

ii. **Account Use.** You must use your Microsoft account to keep it active. This means you must sign in at least once in a five-year period to keep your Microsoft account, and associated Services, active, unless provided otherwise in an offer for a paid portion of the Services. If you don't sign in during this time, we will assume your Microsoft account is inactive and will close it for you. Please see section 4(a)(iv)(2) for the consequences of a closed Microsoft account. You must sign into your Outlook.com inbox and your OneDrive (separately) at least once in a one-year period, otherwise we will close your Outlook.com inbox and your OneDrive for you. If we reasonably suspect that your Microsoft account or Skype account is being used by a third party fraudulently (for example, as a result of an account compromise), Microsoft may suspend your account until you can reclaim ownership. If you are having trouble accessing your Microsoft account, please visit this website: <http://go.microsoft.com/fwlink/?LinkId=238656>. To manage your Skype account, you must "Sign In" at www.skype.com.

iii. **Kids and Accounts.** By using the Services, you represent that you have either reached the age of "majority" where you live or have valid parent or legal guardian consent to be bound by these Terms. If you do not know whether you have reached the age of majority where you live, or do not understand this section, please ask your parent or legal guardian for help before you create a Microsoft account or Skype account. If you are the parent or legal

guardian of a minor that creates a Microsoft account or Skype account, you accept these Terms on the minor's behalf and are responsible for all use of the Microsoft account, Skype account, or Services, including purchases, whether the minor's account is now open or created later.

iv. **Closing Your Account.**

1. You can cancel specific Services or close your Microsoft account or Skype account at any time and for any reason. To close your Microsoft account, please visit <http://go.microsoft.com/fwlink/p/?linkid=618278>. When you ask us to close your Microsoft account, we will put it in a suspended state for 60 days just in case you change your mind. After that 60 day period, your Microsoft account will be closed. See section 4(a)(iv) (2) below for a detailed explanation as to what happens when your Microsoft account is closed. Logging back in during that 60 day period will reactivate your Microsoft account. To cancel your Skype account please submit a support request to <http://go.microsoft.com/fwlink/p/?linkid=618280>.

2. If your Services are canceled or your Microsoft account or Skype account is closed (whether by you or us), a few things happen. First, your right to use the Services stops immediately and your license to use the software related to the Services ends. Second, we'll delete Data or Your Content associated with your Microsoft account or Skype account or will otherwise disassociate it from you and your Microsoft account or Skype account (unless we are required by law to keep it). You should have a regular backup plan as Microsoft won't be able to retrieve Your Content or Data once your account is closed. Third, you may lose access to material or products you've acquired.

b. **Additional Equipment/Data Plans.** To use many of the Services, you'll need an internet connection and/or data/cellular plan. You might also need additional equipment, like a headset, camera or microphone. You are responsible for providing all connections, plans, and/or equipment needed to use the Services and for paying the fees charged by the provider(s) of your connections, plans, and equipment. Those fees are in addition to any fees you pay us for the Services and we will not reimburse you for such fees. Check with your provider(s) to determine if there are any such fees that may apply to you.

c. **Service Notifications.** When there's something important to tell you about a Service you use, we'll send you Service notifications to the email associated with your Microsoft account or, for Skype notifications, your Skype account. If you authorized use of your phone number for your Microsoft account or Skype account, then we may send Service notifications to you via SMS (text message). **Data or messaging rates may apply when receiving notifications via SMS.**

d. **Support.** Customer support for the Services is available at <http://support.microsoft.com>.

[↑Top of page](#)

Using Third-Party Apps and Services

5. **Using Third-Party Apps and Services.** Our Services may allow you to access or acquire

products, services, websites, links, content, material, games or applications from third parties (companies or people who aren't Microsoft) ("Third-Party Apps and Services"). Many of our Services also help you find Third-Party Apps and Services, and you understand that you are directing our Services to provide Third-Party Apps and Services to you. The Third-Party Apps and Services may also allow you to store Your Content or Data with the publisher, provider, or operator of the Third-Party Apps and Services. The Third-Party Apps and Services may present you with a privacy policy or require you to accept additional terms of use before you can install or use the Third-Party App or Service. See section 14(b) for additional terms for applications acquired through the Office Store, the Xbox Store or the Windows Store. You should review any additional terms and privacy policies before acquiring or using any Third-Party Apps and Services. Any additional terms do not modify any of these Terms. You are responsible for your dealings with third parties. Microsoft does not license any intellectual property to you as part of any Third-Party Apps and Services and is not responsible for information provided by third parties.

[↑Top of page](#)

Service Availability

6. Service Availability.

- a. The Services, Third-Party Apps and Services, or material or products offered through the Services may be unavailable from time to time, may be offered for a limited time, or may vary depending on your region or device. If you change the location associated with your Microsoft account, you may need to re-acquire the material or applications that were available to you and paid for in your previous region.
- b. We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you've stored. We recommend that you regularly backup Your Content that you store on the Services or store using Third-Party Apps and Services.

[↑Top of page](#)

Updates to the Services or Software, and Changes to These Terms

7. Updates to the Services or Software, and Changes to These Terms.

- a. We may change these Terms at any time, and we'll tell you when we do. Using the Services after the changes become effective means you agree to the new terms. If you don't agree to the new terms, you must stop using the Services, close your Microsoft account and/or Skype account and, if you are a parent or guardian, help your minor child close his or her Microsoft account or Skype account.
- b. Sometimes you'll need software updates to keep using the Services. We may automatically check your version of the software and download software updates

or configuration changes, including those that prevent you from accessing the Services, playing counterfeit games, or using unauthorized hardware peripheral devices. You may also be required to update the software to continue using the Services. Such updates are subject to these Terms unless other terms accompany the updates, in which case, those other terms apply. Microsoft isn't obligated to make any updates available and we don't guarantee that we will support the version of the system for which you licensed the software.

c. Additionally, there may be times when we need to remove or change features or functionality of the Service or stop providing a Service or access to Third-Party Apps and Services altogether. Except to the extent required by applicable law, we have no obligation to provide a re-download or replacement of any material, Digital Goods (defined in section 14(b)(v)), or applications previously purchased. We may release the Services or their features in a beta version, which may not work correctly or in the same way the final version may work.

d. So that you can use material protected with digital rights management (DRM), like some music, games, movies and more, DRM software may automatically contact an online rights server and download and install DRM updates.

[↑Top of page](#)

Software License

8. **Software License.** Unless accompanied by a separate Microsoft license agreement (for example, if you are using a Microsoft application that is included with and a part of Windows, then the Windows Software License Terms govern such software), and except as provided in section 14(b)(i) below for applications available through the Office Store, the Windows Store or the Xbox Store, any software provided by us to you as part of the Services is subject to these Terms.

- a. If you comply with these Terms, we grant you the right to install and use one copy of the software per device on a worldwide basis for use by only one person at a time as part of your use of the Services. The software or website that is part of the Services may include third-party code. Any third-party scripts or code, linked to or referenced from the software or website, are licensed to you by the third parties that own such code, not by Microsoft. Notices, if any, for the third-party code are included for your information only.
- b. The software is licensed, not sold, and Microsoft reserves all rights to the software not expressly granted by Microsoft, whether by implication, estoppel, or otherwise. This license does not give you any right to, and you may not:
 - i. circumvent or bypass any technological protection measures in or relating to the software or Services;
 - ii. disassemble, decompile, decrypt, hack, emulate, exploit, or reverse engineer any software or other aspect of the Services that is included in or accessible through the Services, except and only to the extent that the applicable copyright law expressly permits doing so;
 - iii. separate components of the software or Services for use on different devices;
 - iv. publish, copy, rent, lease, sell, export, import, distribute, or lend the software or the Services, unless Microsoft expressly authorizes you to do so;
 - v. transfer the software, any software licenses, or any rights to access or use

the Services;

vi. use the Services in any unauthorized way that could interfere with anyone else's use of them or gain access to any service, data, account, or network;

vii. enable access to the Services or modify any Microsoft-authorized device (e.g., Xbox One, Xbox 360, Microsoft Surface, etc.) by unauthorized third-party applications.

[↑Top of page](#)

Payment Terms

9. **Payment Terms.** If you purchase a Service, then these payment terms apply to your purchase and you agree to them.

a. **Charges.** If there is a charge associated with a portion of the Services, you agree to pay that charge. The price stated for the Services excludes all applicable taxes and currency exchange settlements, unless stated otherwise. The price for Skype paid products includes a charge for the product and a charge for taxes. You are solely responsible for paying such taxes or other charges. Taxes are calculated based on your location at the time your Microsoft or Skype account was registered. We may suspend or cancel the Services if we do not receive an on time, full payment from you. Suspension or cancellation of the Services for non-payment could result in a loss of access to and use of your account and its content. Connecting to the Internet via a corporate or other private network which masks your location may cause charges to be different from those displayed for your actual location.

b. **Your Billing Account.** To pay the charges for a Service, you will be asked to provide a payment method at the time you sign up for that Service. You can access and change your billing information and payment method on the [Microsoft account management website](#) and for your Skype billing account by signing into your account at www.skype.com. Additionally, you agree to permit Microsoft to use any updated account information regarding your selected payment method provided by your issuing bank or the applicable payment network. You agree to keep your billing account and contact information current at all times. Changes made to your billing account will not affect charges we submit to your billing account before we could reasonably act on your changes to your billing account.

c. **Billing.** By providing Microsoft with a payment method, you (i) represent that you are authorized to use the payment method that you provided and that any payment information you provide is true and accurate; (ii) authorize Microsoft to charge you for the Services or available content using your payment method; and (iii) authorize Microsoft to charge you for any paid feature of the Services that you choose to sign up for or use while these Terms are in force. We may bill you (a) in advance; (b) at the time of purchase; (c) shortly after purchase; or (d) on a recurring basis for subscription Services. Also, we may charge you up to the amount you have approved, and we will notify you in advance of any change in the amount to be charged for recurring subscription Services. We may bill you at the same time for more than one of your prior billing periods for amounts that haven't previously been processed.

d. **Recurring Payments.** When you purchase the Services on a subscription basis (e.g., monthly, every 3 months or annually (as applicable)), you acknowledge and

agree that you are authorizing recurring payment, and payments shall be made to Microsoft by the method you have chosen at the recurring intervals chosen by you, until the subscription for that Service is terminated by you or by Microsoft. By authorizing recurring payments, you are authorizing Microsoft to process such payments as either electronic debits or fund transfers, or as electronic drafts from your designated account (in the case of Automated Clearing House or similar payments), or as charges to your designated account (in the case of credit card or similar payments) (collectively, "Electronic Payments"). Subscription fees are generally billed or charged in advance of the applicable subscription period. If any payment is returned unpaid or if any credit card or similar transaction is rejected or denied, Microsoft or its service providers reserve the right to collect any applicable return item, rejection or insufficient funds fee and to process any such payment as an Electronic Payment.

e. Automatic Renewal. Provided that automatic renewals are allowed in your state, we will inform you by email before automatically renewing your Services, unless purchased on a subscription basis. Once we have informed you that the Services will be automatically renewed, we may automatically renew your Services and charge you the then current price for the renewal term. We will also remind you that we will bill your chosen payment method for the Services renewal, whether it was on file on the renewal date or provided later. We will also provide you with instructions on how you may cancel the Services. You must cancel the Services before the renewal date to avoid being billed for the renewal.

f. Online Statement and Errors. Microsoft will provide you with an online billing statement on the [Microsoft account management website](#), where you can view and print your statement. For Skype accounts you can access your online statement by signing into your account at www.skype.com. This is the only billing statement that we provide. If we make an error on your bill, you must tell us within 90 days after the error first appears on your bill. We will then promptly investigate the charge. If you do not tell us within that time, you release us from all liability and claims of loss resulting from the error and we won't be required to correct the error or provide a refund. If Microsoft has identified a billing error, we will correct that error within 90 days.

g. Refund Policy. Unless otherwise provided by law or by a particular Service offer, all purchases are final and non-refundable. If you believe that Microsoft has charged you in error, you must contact us within 90 days of such charge. No refunds will be given for any charges more than 90 days old. We reserve the right to issue refunds or credits at our sole discretion. If we issue a refund or credit, we are under no obligation to issue the same or similar refund in the future. This refund policy does not affect any statutory rights that may apply. For more refund information, please visit our [help topic](#).

h. Canceling the Services. You may cancel a Service at any time, with or without cause. To cancel a Service and request a refund, if you are entitled to one, visit the [Microsoft account management website](#). You can request a refund from Skype using the [Cancellation and Refund form](#). You should refer back to the offer describing the Services as (i) you may not receive a refund at the time of cancellation; (ii) you may be obligated to pay cancellation charges; (iii) you may be obligated to pay all charges made to your billing account for the Services before the date of cancellation; or (iv) you may lose access to and use of your account when you cancel the Services. If you cancel, your access to the Services ends at the end of your current Service period or, if we bill your account on a periodic basis, at the end of the period in which you canceled.

i. **Trial-Period Offers.** If you are taking part in any trial-period offer, you must cancel the trial Service(s) by the end of the trial period to avoid incurring new charges, unless we notify you otherwise. If you do not cancel the trial Service(s) by the end of the trial period, we may charge you for the Service(s).

j. **Promotional Offers.** From time to time, Microsoft may offer Services for a trial period during which Microsoft will not charge you for the Services. Microsoft reserves the right to charge you for such Services (at the normal rate) in the event that Microsoft determines (in its reasonable discretion) that you are breaching the terms and conditions of the offer.

k. **Price Changes.** We may change the price of the Services at any time and if you have a recurring purchase, we will notify you by email at least 15 days before the price change. If you do not agree to the price change, you must cancel and stop using the Services before the price change takes effect. If there is a fixed term and price for your Service offer, that price will remain in force for the fixed term.

l. **Payments to You.** If we owe you a payment, then you agree to timely and accurately provide us with any information we need to get that payment to you. You are responsible for any taxes and charges you may incur as a result of this payment to you. You must also comply with any other conditions we place on your right to any payment. If you receive a payment in error, we may reverse or require return of the payment. You agree to cooperate with us in our efforts to do this. We may also reduce the payment to you without notice to adjust for any previous overpayment.

m. **Gift Cards.** Redemption and use of gift cards (other than Skype gift cards) are governed by the [Microsoft Gift Card Terms and Conditions](#). Information on Skype gift cards is available on [Skype's Help page](#).

[↑Top of page](#)

Contracting entity, choice of law, jurisdiction

10. **Contracting Entity.** For use of free, consumer Skype-branded Services, you're contracting with, and all references to "Microsoft" in these Terms shall mean, Skype Software S.à.r.l, 23 – 29 Rives de Clausen, L-2165 Luxembourg, and for paid, consumer Skype-branded Services, you're contracting with, and all references to "Microsoft" in these Terms shall mean, Skype Communications S.à.r.l, 23 – 29 Rives de Clausen, L-2165 Luxembourg. For all other Services, you're contracting with Microsoft Corporation, One Microsoft Way, Redmond, WA 98052, U.S.A.

11. **Choice of Law and Place to Resolve Disputes.** If you live in (or, if a business, your principal place of business is in) the United States, the laws of the state where you live govern all claims, regardless of conflict of law principles, except that the Federal Arbitration Act governs all provisions relating to arbitration. You and we irrevocably consent to the exclusive jurisdiction and venue of the state or federal courts in King County, Washington, for all disputes arising out of or relating to these Terms or the Services that are heard in court (excluding arbitration and small claims court).

[↑Top of page](#)

Warranties

12. **Warranties.** MICROSOFT, AND OUR AFFILIATES, RESELLERS, DISTRIBUTORS, AND VENDORS, MAKE NO WARRANTIES, EXPRESS OR IMPLIED, GUARANTEES OR CONDITIONS WITH RESPECT TO YOUR USE OF THE SERVICES. YOU UNDERSTAND THAT USE OF THE SERVICES IS AT YOUR OWN RISK AND THAT WE PROVIDE THE SERVICES ON AN "AS IS" BASIS "WITH ALL FAULTS" AND "AS AVAILABLE." YOU BEAR THE ENTIRE RISK OF USING THE SERVICES. MICROSOFT DOESN'T GUARANTEE THE ACCURACY OR TIMELINESS OF INFORMATION AVAILABLE FROM THE SERVICES. TO THE EXTENT PERMITTED UNDER YOUR LOCAL LAW, WE EXCLUDE ANY IMPLIED WARRANTIES, INCLUDING FOR MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, WORKMANLIKE EFFORT, AND NON-INFRINGEMENT. YOU MAY HAVE CERTAIN RIGHTS UNDER YOUR LOCAL LAW. NOTHING IN THESE TERMS IS INTENDED TO AFFECT THOSE RIGHTS, IF THEY ARE APPLICABLE. YOU ACKNOWLEDGE THAT COMPUTER AND TELECOMMUNICATIONS SYSTEMS ARE NOT FAULT-FREE AND OCCASIONAL PERIODS OF DOWNTIME OCCUR. WE DO NOT GUARANTEE THE SERVICES WILL BE UNINTERRUPTED, TIMELY, SECURE, OR ERROR-FREE OR THAT CONTENT LOSS WON'T OCCUR, NOR DO WE GUARANTEE ANY CONNECTION TO OR TRANSMISSION FROM THE COMPUTER NETWORKS.

[↑Top of page](#)

Limitation of Liability

13. **Limitation of Liability.** If you have any basis for recovering damages (including breach of these Terms), you agree that your exclusive remedy is to recover, from Microsoft or any affiliates, resellers, distributors, Third-Party Apps and Services providers, and vendors, direct damages up to an amount equal to your Services fee for the month during which the breach occurred (or up to \$10.00 if the Services are free). You can't recover any other damages or losses, including, without limitation, direct, consequential, lost profits, special, indirect, incidental, or punitive. These limitations and exclusions apply even if this remedy doesn't fully compensate you for any losses or fails of its essential purpose or if we knew or should have known about the possibility of the damages. To the maximum extent permitted by law, these limitations and exclusions apply to anything or any claims related to these Terms, the Services, or the software related to the Services.

[↑Top of page](#)

Service-Specific Terms

14. **Service-Specific Terms.** The terms before and after section 14 apply generally to all Services. This section contains service-specific terms that are in addition to the general terms.

[↑Top of page](#)

Xbox Live and Microsoft Studios Games and Applications

a. **Xbox Live and Microsoft Studios Games and Applications.**

i. **Personal Noncommercial Use.** Xbox Live, Games for Windows Live and Microsoft Studios games, applications, services and content provided by Microsoft (collectively, the "**Xbox Services**") are only for your personal and noncommercial use.

ii. **Sharing Limited Account Information.** As part of delivering the Xbox Services, we make information pertaining to your gamertag, gameplay, Your Content that you make public, and activity on and usage of any Xbox Service available for the operation and delivery of (a) other Xbox Services and (b) third-party games that use Xbox Services. If you choose to link your Microsoft Xbox Services account with your account on a non-Microsoft service (for example, a non-Microsoft game publisher of Third-Party Apps and Services), you agree that: (a) Microsoft may share limited account information (including without limitation gamertag, gamerscore, game score, game history, and friends list), with that non-Microsoft party as stated in the Microsoft Privacy Statement, and (b) if allowed by your Xbox privacy settings, the non-Microsoft party may also have access to Your Content from in-game communications when you are signed into your account with that non-Microsoft party. Also, if allowed by your Xbox privacy settings, Microsoft can publish your gamertag and games that you've played in email to people on your Xbox friends list.

iii. **Your Content.** As part of building the Xbox Services community, you grant to Microsoft, its affiliates and sublicensees the right to use, modify, reproduce, distribute, and display Your Content or your name, gamertag, motto, or avatar that you posted for any Xbox Services.

iv. **Game Managers.** Some games may use game managers and hosts. Game managers and hosts are not authorized Microsoft spokespersons. Their views do not necessarily reflect those of Microsoft.

v. **Kids on Xbox.** If you are a minor using Xbox Live, your parent or guardian may have control over many aspects of your account and may receive reports about your use of Xbox Live.

vi. **Game Currency or Virtual Goods.** The Services may include a virtual, game currency (like gold, coins or points) that may be purchased from Microsoft using actual monetary instruments if you have reached the age of "majority" where you live. The Services may also include virtual, digital items or goods that may be purchased from Microsoft using actual monetary instruments or using game currency. Game currency and virtual goods may never be redeemed for actual monetary instruments, goods or other items of monetary value from Microsoft or any other party. Other than a limited, personal, revocable, non-transferable, non-sublicensable license to use the game currency and virtual goods in the Services only, you have no right or title in or to any such game currency or virtual goods appearing or originating in the Services, or any other attributes associated with use of the Services or stored within the Services. Microsoft may at any time regulate, control, modify and/or eliminate the game currency and/or virtual goods as it sees fit in its sole

discretion.

[↑Top of page](#)

Store

b. **Store.** "Store" refers to a Service that allows you to browse, download, purchase, and rate and review applications (the term "application" includes games) and other digital content. These Terms cover use of Office Store, Xbox Store and Windows Store. "Office Store" means a Store for Office products and apps for Office, SharePoint, Exchange, Access and Project (2013 versions or later). "Windows Store" means a Store for Windows devices such as phone, PC and tablet, or any other experience that is branded Windows Store. "Xbox Store" means a Store for Xbox ONE and Xbox 360 consoles, or any other experience that is branded Xbox Store.

i. **License Terms.** We will identify the publisher of each application available in the relevant Store. The Standard Application License Terms ("**SALT**") at the end of these Terms are an agreement between you and the application publisher setting forth the license terms that apply to your use of an application you download through the Windows Store or the Xbox Store, unless different license terms are provided with the application. Applications downloaded through the Office Store are not governed by the SALT and have separate license terms that apply. Section 5 of these Terms applies to any Third-Party Apps and Services acquired through a Store.

ii. **Updates.** Microsoft will automatically check for and download updates to your applications, even if you're not signed into the relevant Store. You can change your Store or system settings if you prefer not to receive automatic updates to Store apps. However, certain Office Store apps that are entirely or partly hosted online may be updated at any time by the app developer and may not require your permission to update.

iii. **Private Store Experiences.** Some business organizations may provide access to a "private store" experience for their employees, contractors, and agents. These Terms do not cover use of a private store (if any); these Terms only cover your personal, noncommercial use of the Stores.

iv. **Ratings and Reviews.** If you rate or review an application in a Store, you may receive email from Microsoft containing content from the publisher of the application. Any such email comes from Microsoft; we do not share your email address with any publishers of applications you acquire through the Store.

v. **When you obtain music, video or books directly from Microsoft, the following terms apply:** Through the Windows Store and/or the Xbox Store, Microsoft may enable you to obtain, listen to, view, and/or read (as the case may be) music, images, video, text, or other material ("**Digital Goods**") that you may get in digital form. The Digital Goods are only for your personal, noncommercial entertainment use. You agree not to redistribute, broadcast, publicly perform or publicly display or transfer any copies of the Digital Goods obtained through any of the Stores. Digital Goods may be owned by Microsoft or by third parties. However, in all circumstances, you understand and acknowledge that your rights with respect to Digital Goods are limited by these Terms, copyright law, and the usage rules located at <http://www.xbox.com/usagerules>. You agree that you will not attempt to

modify any Digital Goods obtained through any of the Stores for any reason whatsoever, including for the purpose of disguising or changing ownership or source of the Digital Goods. Microsoft and/or the owners of the Digital Goods may, from time to time, remove Digital Goods from the Stores without notice.

vi. **Safety Warning.** To avoid possible injury or eye strain, you should take periodic breaks from use of applications available through a Store, especially if you feel any pain or fatigue resulting from usage. A very small percentage of people may experience seizures when exposed to certain visual images like flashing lights or patterns that may appear in applications. Even people with no history of seizures may have an undiagnosed condition that can cause these seizures. Symptoms may include lightheadedness, altered vision, twitching, jerking or shaking of limbs, disorientation, confusion, loss of consciousness, or convulsions. Immediately stop using and consult a doctor if you experience any of these symptoms, or consult a doctor before using the applications if you've ever suffered symptoms linked to seizures. Parents should monitor their children's use of applications for signs of symptoms.

[↑Top of page](#)

Microsoft Family

c. **Microsoft Family.** Parents and kids can use Microsoft Family to build trust based on a shared understanding of what behaviors, websites, apps, games, physical locations, and spending is right in their family. Parents can create a "Family" by going to <https://account.microsoft.com/family> (or by following the instructions on their Windows device or Xbox console) and inviting kids or other parents to join. There are many features available to Family members, so please carefully review the information provided when you agree to create or join a "Family." By creating or joining a "Family," you represent that you will use the "Family" in accordance with its purpose and won't use it in an unauthorized way to unlawfully gain access to another person's information.

[↑Top of page](#)

Skype

d. **Skype.**

i. **No Access to Emergency Services.** There are important differences between traditional telephone services and Skype. Skype is not required to offer access to Emergency Services under any applicable local and/or national rules, regulations, or law. Skype's software and products are not intended to support or carry emergency calls to any type of hospitals, law enforcement agencies, medical care units or any other kind of services that connect a user to emergency services personnel or public safety answering points ("**Emergency Services**"). You acknowledge and agree that: (i) it is your responsibility to purchase traditional wireless (mobile) or fixed-line telephone services that offer access to Emergency Services, and (ii) Skype is not a replacement for your primary telephone service.

ii. **APIs or Broadcasting.** If you want to use Skype in connection with any broadcast, you must comply with the "Broadcast TOS" at <http://www.skype.com/go/legal.broadcast>. If you want to use any application program interface ("API") exposed or made available by Skype you must comply with the applicable licensing terms, which are available at www.skype.com/go/legal.

iii. **Fair Use Policies.** Fair usage policies may apply to your use of Skype. Please review these policies which are designed to protect against fraud and abuse and may place limits on the type, duration or volume of calls or messages that you are able to make. These policies are incorporated in these Terms by reference. You can find these policies at: <http://www.skype.com/go/terms.fairusage/>

iv. **Mapping.** Skype contains features that allow you to submit information to, or plot yourself on a map using, a mapping service. By using those features, you agree to these Terms and the Google Maps terms available at http://www.google.com/intl/en_ALL/help/terms_maps.html.

v. **Government Users.** If you wish to use a business account and/or Skype Manager on behalf of the U.S. Government or an agency of the U.S. Government, these Terms do not apply to that use. For applicable terms and/or further information, please contact usgovusers@skype.net.

vi. **Personal/Noncommercial Use.** The use of Skype is for your personal and noncommercial use. You are permitted to use your personal Skype account at work for your own business communications.

vii. **Skype Number/Skype To Go.** If Skype provides you with a Skype Number or Skype To Go number, you agree that you do not own the number or have a right to retain that number forever.

viii. **Skype Manager.** A "Managed Account" is a Skype account that is created and managed by you, acting as an individual administrator of your Skype Manager and not as a business entity. You may appoint additional administrators to your Skype Manager subject to their acceptance of these Terms. You are responsible for all use of your Managed Accounts. Managed Accounts are for individual use only and may not be shared. If you allocate Skype Numbers to a Managed Account, you are responsible for compliance with any requirements related to the residency or location of your Managed Account users. If you choose to delete a Managed Account, any allocated subscriptions or unclaimed Skype Credit or Skype Numbers may be lost and Your Content or material associated with the deleted Managed Account will no longer be accessible by you. Skype reserves the right to cancel Managed Accounts that have been inactive for more than one year. You agree to process any personal information of your Managed Account users in accordance with all applicable data protection laws.

ix. **Skype Charges.** Skype paid products are sold to you by Skype Communications S.à.r.l, however the seller-of-record accountable for taxes is Skype Communications US Corporation. Taxes means the amount of taxes, regulatory fees, surcharges or other fees that we are required to collect from you and must pay to any United States (federal, state or local) or foreign government, agency, commission or quasi-governmental body as a result of our provision of Skype paid products to you. These taxes are listed at www.skype.com/go/ustax. All prices for Skype paid products are inclusive of a

charge for your product and a charge for taxes, unless otherwise stated. The charges payable for calling phones outside of a subscription consist of a connection fee (charged once per call) and a per-minute rate as set out at www.skype.com/go/allrates. Call charges will be deducted from your Skype Credit balance. Skype may change its calling rates at any time without notice to you by posting such change at www.skype.com/go/allrates. The new rate will apply to your next call after publication of the new rates. Please check the latest rates before you make your call. Fractional call minutes and fractional cent charges will be rounded up to the next whole unit.

x. **Skype Credit.** Skype does not guarantee that you will be able to use your Skype Credit balance to purchase all Skype paid products. If you do not use your Skype Credit for a period of 180 days, Skype will place your Skype Credit on inactive status. You can reactivate the Skype Credit by following the reactivation link at <http://www.skype.com/go/store.reactivate.credit>. You can enable the Auto Recharge feature when you buy Skype Credit by ticking the appropriate box. If enabled, your Skype Credit balance will be recharged with the same amount and by your chosen payment method every time your Skype account balance goes below the threshold set by Skype from time to time. If you purchased a subscription with a payment method other than credit card, PayPal or Moneybookers (Skrill), and you have enabled Auto-Recharge, your Skype Credit balance will be recharged with the amount necessary to purchase your next recurring subscription. You can disable Auto-Recharge at any time by accessing and changing your settings in your Skype account.

[↑Top of page](#)

Bing and MSN

e. Bing and MSN.

i. **Bing and MSN Materials.** The articles, text, photos, maps, videos, video players, and third-party material available on Bing and MSN are for your noncommercial, personal use only. Other uses, including downloading, copying, or redistributing these materials, are permitted only to the extent specifically authorized by Microsoft or rights holders, or allowed by applicable copyright law. Microsoft or other rights holders reserve all rights to the material not expressly granted by Microsoft under the license terms, whether by implication, estoppel, or otherwise.

ii. **Bing Maps.** You may not use Bird's eye imagery of the United States, Canada, Mexico, New Zealand, Australia or Japan for governmental use without our separate written approval.

[↑Top of page](#)

Bing Rewards

iii. **Bing Rewards.** Bing Rewards (the "**Program**") enables you to earn redeemable credits for your searches as well as through offers from other Microsoft services. A search is the act of an individual user manually entering

text for the good faith purpose of obtaining Bing search results for such user's own research purposes and does not include any query entered by a bot, macro, or other automated or fraudulent means of any kind ("**Search**"). Microsoft in its sole discretion determines what constitutes a Search that qualifies for credits. Your earned credits, whether through Search or other offers, can be redeemed for items, discounts, or donations to nonprofit organizations ("**Rewards**") in the [redemption center](#). For more information see the [Frequently Asked Questions](#) ("**FAQ**").

1. *Program Requirements.* You need a valid Microsoft account and your devices must meet the [minimum system requirements](#). The Program is open to users who reside in the 50 United States or the District of Columbia and who are at least 13 years of age. Individuals can have no more than one Program account and households are limited to five accounts.

2. *Credits.* Except for donating your credits to a nonprofit organization listed in the redemption center, you cannot transfer credits. Credits are not your personal property, and you may not obtain any cash or money in exchange for them. Microsoft may limit the quantity of credits or Rewards per person, per household, or over a set period (e.g., a day). You may redeem no more than 55,000 credits per calendar year in the Program. Credits earned in the Program are not valid in, and may not be used in combination with, any other program offered by Microsoft or third parties. Unredeemed credits expire if you do not earn any credits for 180 days.

3. *Rewards.* You may redeem your credits by visiting the [redemption center](#) or you may contribute credits to a listed nonprofit organization. There may be a limited number of a particular Reward available, and those Rewards will be delivered on a first-come, first-served basis. You may be required to provide additional information, like your mailing address and a telephone number (other than a VOIP or toll-free number), and you may also be asked to enter a fraud-prevention code or sign additional legal documents in order to redeem credits for Rewards. Once you order a Reward, you cannot cancel it or return it for a refund of credits. If you order a Reward that is out of stock or unavailable for other reasons Microsoft determines in its sole discretion, we may substitute a Reward of comparable value or refund your credits. Some Rewards may have age eligibility requirements. You are responsible for all federal, state, and local taxes and any other costs of accepting and using the Reward. Rewards will be emailed to the email address you provide when ordering your Reward, so keep your email address up to date. Rewards that are undeliverable will not be reissued and are therefore forfeited. Rewards are not for resale.

4. *Cancelling Your Participation in the Program.* Microsoft reserves the right to cancel the Program account of a specific user at our discretion. Such cancellation or suspension may be without cause and we are under no obligation to provide a reason. Upon Program cancellation (by you or us) or if the Program is suspended, you will have 90 days to redeem your credits; otherwise, those credits will be forfeited. At the point of cancellation, your right to use the Program and accrue future credits ends.

5. *Other Conditions.* Microsoft reserves the right to disqualify you; disable your access to the Program or your Rewards account; and/or withhold credits, Rewards and charitable contributions, if Microsoft believes you are tampering with or abusing any aspect of the Program or may be engaging

in activities that violate these Terms.

[↑Top of page](#)

Cortana

f. **Cortana.** Cortana is Microsoft's personal assistant Service. Cortana provides information for your planning purposes only and you should exercise your own independent judgment when reviewing and relying on this information. Microsoft does not guarantee the accuracy, completeness, reliability, availability or timeliness of inferences and personalized experiences provided by Cortana. Microsoft is not responsible if a Cortana communication management feature delays or prevents you from reviewing or sending a communication.

[↑Top of page](#)

Outlook.com

g. **Outlook.com.** The Outlook.com (or @msn, @hotmail, or @live) email address that you use to create your Microsoft account will be unique to you for as long as your Outlook.com inbox or Microsoft account is still active. In the event your Outlook.com inbox or Microsoft account is closed either by you or by Microsoft pursuant to these Terms, the email address or username may be recycled into our system and assigned to another user.

[↑Top of page](#)

Office-based Services

h. **Office-based Services.** Office consumer-based services, applications, or products (including Sway and OneNote) are for your personal, noncommercial use, unless you have commercial use rights under a separate agreement with Microsoft.

[↑Top of page](#)

HealthVault

i. **HealthVault.** HealthVault is intended for you to store your personal health-related information and information about other people (such as your family) with their consent. HealthVault accounts are not for use by healthcare providers or for any other commercial or non-personal purpose. The information in your account may not always be accurate or up-to-date and should be viewed by any health care provider as informational only. The HealthVault Service does not hold records for healthcare providers or other medical or case management purposes. For example,

HealthVault records are not designated record sets as defined under U.S. regulations. If a healthcare provider decides to include any data made available from HealthVault in its records, it should store a copy in its own system. If there is a co-custodian of a record in your account (because one of you invited the other), you acknowledge that the co-custodian has full control over that record and may cancel your access to the record, manage other peoples' access to the record, and view the record's data including how and when the record is used. Microsoft does not support non-Microsoft credentials (such as Facebook and OpenID), so HealthVault customer support will not be able to help with sign-in issues for those. If you lose your sign-in credentials, or if the account where you got your credentials closes, you will not be able to recover your stored data. To help maintain continued access, we suggest you use more than one sign-in credential with your HealthVault account. Microsoft does not endorse or control, and is not responsible for, the operation, support, or security of non-Microsoft credentials you may use.

[↑Top of page](#)

Binding Arbitration and Class Action Waiver

15. Binding Arbitration and Class Action Waiver If You Live In (or If a Business Your Principal Place of Business Is In) the United States. We hope we never have a dispute, but if we do, you and we agree to try for 60 days to resolve it informally. If we can't, you and we agree to **binding individual arbitration before the American Arbitration Association ("AAA") under the Federal Arbitration Act ("FAA"), and not to sue in court in front of a judge or jury.** Instead, a neutral arbitrator will decide and the arbitrator's decision will be final except for a limited right of appeal under the FAA. **Class action lawsuits, class-wide arbitrations, private attorney-general actions, and any other proceeding where someone acts in a representative capacity aren't allowed. Nor is combining individual proceedings without the consent of all parties.**"We," "our," and "us" includes Microsoft, Skype (see section 10) and Microsoft's affiliates and, if you use Skype Pay by Mobile, your mobile phone carrier.

a. Disputes Covered—Everything Except IP. The term "dispute" is as broad as it can be. It includes any claim or controversy between you and us concerning the Services, the software related to the Services, the Services' or software's price, your Microsoft account, your Skype account, or these Terms, under any legal theory including contract, warranty, tort, statute, or regulation, **except disputes relating to the enforcement or validity of your, your licensors', our, or our licensors' intellectual property rights.**

b. Mail a Notice of Dispute First. If you have a dispute and our customer service representatives can't resolve it, send a Notice of Dispute by U.S. Mail to **Microsoft Corporation, ATTN: LCA ARBITRATION, One Microsoft Way, Redmond, WA 98052-6399, U.S.A.** (or to your mobile phone carrier at its principal place of business in the United States marked ATTN: Legal Department). Tell us your name, address, how to contact you, what the problem is, and what you want. A form is available at <http://go.microsoft.com/fwlink/?LinkId=245499>. We'll do the same if we have a dispute with you. After 60 days, you or we may start an arbitration if the dispute is unresolved.

c. Small Claims Court Option. Instead of mailing a Notice of Dispute, you may sue

us in small claims court in your county of residence (or if a business your principal place of business) or King County, Washington, U.S.A. if you meet the court's requirements. We hope you'll mail a Notice of Dispute and give us 60 days to try to work it out, but you don't have to before going to small claims court.

d. **Arbitration Procedure.** The AAA will conduct any arbitration under its Commercial Arbitration Rules (or if you are an individual and use the Services for personal or household use, or if the value of the dispute is \$75,000 or less whether or not you are an individual or how you use the Services, its Consumer Arbitration Rules). For more information, see www.adr.org or call 1-800-778-7879. To start an arbitration, submit the form available at <http://go.microsoft.com/fwlink/?LinkId=245497> to the AAA and mail a copy to us. In a dispute involving \$25,000 or less, any hearing will be telephonic unless the arbitrator finds good cause to hold an in-person hearing instead. Any in-person hearing will take place in your county of residence (or if a business your principal place of business) or our principal place of business—King County, Washington if your dispute is with Microsoft. You choose. The arbitrator may award the same damages to you individually as a court could. The arbitrator may award declaratory or injunctive relief only to you individually to satisfy your individual claim.

e. **Arbitration Fees and Payments.**

i. **Disputes Involving \$75,000 or Less.** We will promptly reimburse your filing fees and pay the AAA's and arbitrator's fees and expenses. If you reject our last written settlement offer made before the arbitrator was appointed, your dispute goes all the way to an arbitrator's decision (called an "award"), and the arbitrator awards you more than this last written offer, we will: (i) pay the greater of the award or \$1,000; (ii) pay your reasonable attorney's fees, if any; and (iii) reimburse any expenses (including expert witness fees and costs) that your attorney reasonably accrues for investigating, preparing, and pursuing your claim in arbitration. The arbitrator will determine the amount of fees, costs, and expenses unless you and we agree on them.

ii. **Disputes Involving More than \$75,000.** The AAA rules will govern payment of filing fees and the AAA's and arbitrator's fees and expenses.

iii. **Disputes Involving Any Amount.** If you start an arbitration, we won't seek our AAA or arbitrator's fees and expenses, or your filing fees we reimbursed, unless the arbitrator finds the arbitration frivolous or brought for an improper purpose. If we start an arbitration, we will pay all filing, AAA, and arbitrator's fees and expenses. We won't seek our attorney's fees or expenses from you in any arbitration. Fees and expenses are not counted in determining how much a dispute involves.

f. **Conflict with AAA Rules.** These Terms govern to the extent they conflict with the AAA's Commercial Arbitration Rules or Consumer Arbitration Rules.

g. **Must File Within One Year.** You and we must file in small claims court or arbitration any claim or dispute (except intellectual property disputes—see section 15.a) within one year from when it first could be filed. Otherwise, it's permanently barred.

h. **Rejecting Future Arbitration Changes.** You may reject any change we make to section 15 (except address changes) by sending us notice within 30 days of the change by U.S. Mail to the address in section 15.b. If you do, the most recent version of section 15 before the change you rejected will apply.

i. **Severability.** If the class action waiver is found to be illegal or unenforceable as to all or some parts of a dispute, then those parts won't be arbitrated but will proceed in court, with the rest proceeding in arbitration. If any other provision of section 15 is found to be illegal or unenforceable, that provision will be severed but the rest of section 15 still applies.

j. **Mobile Phone Carrier as Third-Party Beneficiary.** If you use Skype Pay by Mobile, your mobile phone carrier is a third-party beneficiary of your agreement with Microsoft and Skype to resolve disputes through informal negotiation and arbitration. Your mobile phone carrier agrees to do everything Microsoft and Skype agree to do in section 15.

[↑Top of page](#)

Miscellaneous

16. **Miscellaneous.** This section, and sections 1, 9 (for amounts incurred before the end of these Terms), 10, 11, 12, 13, 15, and those that by their terms apply after the Terms end will survive any termination or cancellation of these Terms. We may assign these Terms, in whole or in part, at any time without notice to you. You may not assign your rights or obligations under these Terms or transfer any rights to use the Services. This is the entire agreement between you and Microsoft for your use of the Services. It supersedes any prior agreements between you and Microsoft regarding your use of the Services. All parts of these Terms apply to the maximum extent permitted by relevant law. If a court or arbitrator holds that we can't enforce a part of these Terms as written, we may replace those terms with similar terms to the extent enforceable under the relevant law, but the rest of these Terms won't change. Section 15(i) says what happens if parts of section 15 (arbitration and class action waiver) are found to be illegal or unenforceable. Section 15(i) prevails over this section if inconsistent with it. Except for Section 15 (arbitration and class action waiver) these Terms are solely for your and our benefit; they aren't for the benefit of any other person, except for Microsoft's successors and assigns.

17. **Export Laws.** You must comply with all domestic and international export laws and regulations that apply to the software and/or Services, which include restrictions on destinations, end users, and end use. For further information on geographic and export restrictions, visit <http://go.microsoft.com/fwlink/?linkid=141397> and <http://www.microsoft.com/exporting>.

18. **Unsolicited Ideas.** Microsoft does not consider or accept unsolicited proposals or ideas, including without limitation ideas for new products, technologies, promotions, product names, product feedback and product improvements ("**Unsolicited Feedback**"). If you send any Unsolicited Feedback to Microsoft through the Services or otherwise, you acknowledge and agree that Microsoft shall not be under any obligation of confidentiality with respect to the Unsolicited Feedback.

[↑Top of page](#)

NOTICES

Notices and procedure for making claims of intellectual property infringement.

Microsoft respects the intellectual property rights of third parties. If you wish to send a notice of intellectual property infringement, including claims of copyright infringement, please use our procedures for submitting [Notices of Infringement](#). **ALL INQUIRIES NOT RELEVANT TO THIS PROCEDURE WILL NOT RECEIVE A RESPONSE.**

Microsoft uses the processes set out in Title 17, United States Code, Section 512 to respond to notices of copyright infringement. In appropriate circumstances, Microsoft may also disable or terminate accounts of users of Microsoft services who may be repeat infringers.

Notices and procedures regarding intellectual property concerns in advertising. Please review our [Intellectual Property Guidelines](#) regarding intellectual property concerns on our advertising network.

Copyright and trademark notices. The Services are copyright © 2015 Microsoft Corporation and/or its suppliers, One Microsoft Way, Redmond, WA 98052, U.S.A. All rights reserved. Microsoft and the names, logos, and icons of all Microsoft products, software, and services may be either [trademarks or registered trademarks of Microsoft](#) in the United States and/or other countries. The names of actual companies and products may be the trademarks of their respective owners. Any rights not expressly granted in these Terms are reserved. Certain software used in certain Microsoft website servers is based in part on the work of the Independent JPEG Group. Copyright © 1991-1996 Thomas G. Lane. All rights reserved. "gnuplot" software used in certain Microsoft website servers is copyright © 1986-1993 Thomas Williams, Colin Kelley. All rights reserved.

Medical notice. Microsoft does not provide medical or any other health care advice, diagnosis, or treatment. Always seek the advice of your physician or other qualified health care provider with any questions you may have regarding a medical condition, diet, fitness, or wellness program. Never disregard professional medical advice or delay in seeking it because of information you accessed on or through the Services.

Stock quotes and index data (including index values). © 2013 Morningstar, Inc. All Rights Reserved. The information contained herein: (1) is proprietary to Morningstar and/or its content providers; (2) may not be copied or distributed; and (3) is not warranted to be accurate, complete or timely. Neither Morningstar nor its content providers are responsible for any damages or losses arising from any use of this information. Past performance is no guarantee of future results.

You may not use any of the Dow Jones IndexesSM, index data, or the Dow Jones marks in connection with the issuance, creation, sponsorship, trading, marketing, or promotion of any financial instruments or investment products (for example, derivatives, structured products, investment funds, exchange-traded funds, investment portfolios, etc., where the price, return and/or performance of the instrument or investment product is based on, related to, or intended to track any of the Indexes or a proxy for any of the Indexes) without a separate written agreement with Dow Jones.

Financial notice. Microsoft isn't a broker/dealer or registered investment advisor under United States federal securities law or securities laws of other jurisdictions and doesn't advise individuals as to the advisability of investing in, purchasing, or selling securities or other financial products or services. Nothing contained in the Services is an offer or solicitation to buy or sell any security. Neither Microsoft nor its licensors of stock quotes or index data endorse or recommend any particular financial products or services. Nothing in the Services is intended to be professional advice, including but not limited to, investment or tax advice.

Notice about the H.264/AVC, MPEG-4 Visual, and VC-1 Video Standards. The software may include H.264/AVC, MPEG-4 Visual and/or VC-1 codec technology that may be licensed by MPEG LA, L.L.C. This technology is a format for data compression of video

information. MPEG LA, L.L.C. requires this notice:

THIS PRODUCT IS LICENSED UNDER THE H.264/AVC, MPEG-4 VISUAL, AND THE VC-1 PATENT PORTFOLIO LICENSES FOR THE PERSONAL AND NONCOMMERCIAL USE OF A CONSUMER TO (A) ENCODE VIDEO IN COMPLIANCE WITH THE STANDARDS ("VIDEO STANDARDS") AND/OR (B) DECODE H.264/AVC, MPEG-4 VISUAL, AND VC-1 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NONCOMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE SUCH VIDEO. NONE OF THE LICENSES EXTEND TO ANY OTHER PRODUCT REGARDLESS OF WHETHER SUCH PRODUCT IS INCLUDED WITH THIS SOFTWARE IN A SINGLE ARTICLE. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE THE [MPEG LA WEBSITE](#).

For clarification purposes only, this notice does not limit or inhibit the use of the software provided under these Terms for normal business uses that are personal to that business which do not include (i) redistribution of the software to third parties, or (ii) creation of material with the VIDEO STANDARDS compliant technologies for distribution to third parties.

[↑Top of page](#)

STANDARD APPLICATION LICENSE TERMS

STANDARD APPLICATION LICENSE TERMS

WINDOWS STORE AND XBOX STORE

These license terms are an agreement between you and the application publisher. Please read them. They apply to the software applications you download from the Windows Store or the Xbox Store, including any updates or supplements for the application, unless the application comes with separate terms, in which case those terms apply.

BY DOWNLOADING OR USING THE APPLICATION, OR ATTEMPTING TO DO ANY OF THESE, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THEM, YOU HAVE NO RIGHT TO AND MUST NOT DOWNLOAD OR USE THE APPLICATION.

The application publisher means the entity licensing the application to you, as identified in the Windows Store or Xbox Store.

If you comply with these license terms, you have the rights below.

1. **INSTALLATION AND USE RIGHTS; EXPIRATION.** For applications you download from the Windows Store: (a) you may install and use the application on a Windows device or devices that are affiliated with the Microsoft account that you use to access the Windows Store; and (b) the device limit for the application is displayed in the Store or, for some applications downloaded on the Xbox console, the [Xbox Live Usage Rules](#). For applications you download from the Xbox Store, you may install and use the application on Xbox consoles as described in the [Xbox Live Usage Rules](#). Microsoft reserves the right to modify the Xbox Live Usage Rules at any time.

2. **INTERNET-BASED SERVICES.**

a. **Consent for Internet-based or wireless services.** If the application connects

to computer systems over the Internet, which may include via a wireless network, using the application operates as your consent to the transmission of standard device information (including but not limited to technical information about your device, system, and application software, and peripherals) for Internet-based or wireless services. If other terms are presented in connection with your use of services accessed using the application, those terms also apply.

b. **Misuse of Internet-based services.** You may not use any Internet-based service in any way that could harm it or impair anyone else's use of it or the wireless network. You may not use the service to try to gain unauthorized access to any service, data, account, or network by any means.

3. **SCOPE OF LICENSE.** The application is licensed, not sold. This agreement only gives you some rights to use the application. If Microsoft disables the ability to use the applications on your devices pursuant to your agreement with Microsoft, any associated license rights will terminate. Application publisher reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the application only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the application that only allow you to use it in certain ways. You may not:

- a. Work around any technical limitations in the application.
- b. Reverse engineer, decompile, or disassemble the application, except and only to the extent that applicable law expressly permits, despite this limitation.
- c. Make more copies of the application than specified in this agreement or allowed by applicable law, despite this limitation.
- d. Publish or otherwise make the application available for others to copy.
- e. Rent, lease, or lend the application.
- f. Transfer the application or this agreement to any third party.

4. **DOCUMENTATION.** If documentation is provided with the application, you may copy and use the documentation for personal reference purposes.

5. **TECHNOLOGY AND EXPORT RESTRICTIONS.** The application may be subject to United States or international technology control or export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the technology used or supported by the application. These laws include restrictions on destinations, end users, and end use. For information on Microsoft branded products, go to the [Microsoft exporting website](#).

6. **SUPPORT SERVICES.** Contact the application publisher to determine if any support services are available. Microsoft, your hardware manufacturer and your wireless carrier (unless one of them is the application publisher) aren't responsible for providing support services for the application.

7. **ENTIRE AGREEMENT.** This agreement, any applicable privacy policy, and the terms for supplements and updates are the entire license agreement between you and application publisher for the application.

8. **APPLICABLE LAW.**

- a. **United States and Canada.** If you acquired the application in the United States or Canada, the laws of the state or province where you live (or, if a business, where your principal place of business is located) govern the interpretation of these terms, claims for breach of them, and all other claims (including consumer protection, unfair competition, and tort claims),

regardless of conflict of law principles.

b. Outside the United States and Canada. If you acquired the application in any other country, the laws of that country apply.

9. **LEGAL EFFECT.** This agreement describes certain legal rights. You may have other rights under the laws of your state or country. This agreement doesn't change your rights under the laws of your state or country if the laws of your state or country don't permit it to do so.

10. **DISCLAIMER OF WARRANTY.** The application is licensed "as is," "with all faults," and "as available." You bear the entire risk as to its quality and performance. Should it prove defective, you assume the entire cost of all necessary servicing or repair. The application publisher, on behalf of itself, Microsoft, wireless carriers over whose network the application is provided, and each of our respective affiliates, vendors, agents, and suppliers ("Covered Parties"), gives no express warranties, guarantees, or conditions in relation to the application. You may have additional consumer rights under your local laws that this agreement can't change. To the extent permitted under your local laws, Covered Parties exclude any implied warranties or conditions, including those of merchantability, fitness for a particular purpose, and non-infringement. If your local laws impose a warranty, guarantee or condition even though these terms do not, its duration is limited to 90 days from when you download the application.

11. **LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES.** To the extent not prohibited by law, if you have any basis for recovering damages, you can recover from the application publisher only direct damages up to the amount you paid for the application or \$1.00, whichever is greater. You will not, and waive any right to, seek to recover any other damages, including lost profits and consequential, special, direct, indirect, or incidental damages, from the application publisher.

This limitation applies to:

- Anything related to the application or services made available through the application; and
- Claims for breach of contract, warranty, guarantee or condition; strict liability, negligence, or other tort; violation of a statute or regulation; unjust enrichment; or under any other theory; all to the extent permitted by applicable law.

It also applies even if:

- This remedy doesn't fully compensate you for any losses; or
- The application publisher knew or should have known about the possibility of the damages.

[↑Top of page](#)

Covered Services

The following products, apps and services are covered by the Microsoft Services Agreement, but may not be available in your market.

Account.microsoft.com
Advertising.microsoft.com
Bing

Bing Apps
Bing Desktop
Bing Dictionary
Bing in the Classroom
Bing Input
Bing Maps
Bing Navigation
Bing Reader
Bing Rewards
Bing Search app
Bing Toolbar
Bing Torque
Bing Translator
Bing Webmaster
Bing Wikipedia Browser
Bing.com
Bingplaces.com
Choice.microsoft.com
Citizen Next
Cortana
Default Homepage and New Tab Page on Microsoft Edge
Device Health App
HealthVault
Groove
Maps App
Microsoft account
Microsoft Family
Microsoft Health
Microsoft Translator
Microsoft Wallpaper
Microsoft Xiaolce
MSN Dial Up
MSN Explorer
MSN Food & Drink
MSN Health & Fitness
MSN Money
MSN News
MSN Premium
MSN Sports
MSN Travel
MSN Weather
MSN.com
Next Lock Screen
Office 365 Consumer
Office 365 Home
Office 365 Personal
Office 365 University
Office Online
Office Store
Office Sway
Office.com
OneDrive
OneDrive.com
OneNote

Onenote.com
Outlook.com
Picturesque Lock Screen
Pix Lock
Skype
Skype in the Classroom
Skype Manager
Skype Qik
Skype WiFi
Skype.com
Smart Search
Snipp3t
Spreadsheet Keyboard
Sway.com
Translator
UrWeather
Windows Live Mail
Windows Live Writer
Windows Movie Maker
Windows Photo Gallery
Xbox and Windows Games published by Microsoft
Xbox Live
Xbox Music
Xbox Music Pass
Xbox Video

[↑Top of page](#)

Microsoft

[Contact us](#) [Privacy & cookies](#) [Terms of use](#) [Trademarks](#)
[About our ads](#) © 2015 Microsoft



Try Microsoft EdgeA fast and secure browser that's designed for Windows 10

No thanks [Get started](#)



Microsoft

[Store](#)

[Store home](#)

[Devices](#)

[Microsoft Surface](#)

[PCs & tablets](#)

[Xbox](#)

[Virtual reality](#)

[Accessories](#)

[Windows phone](#)

[Software & Apps](#)

[Office](#)

[Windows](#)

[Professional software](#)

[Windows apps](#)

[Windows phone apps](#)

[Games & Entertainment](#)

[Xbox Games \(disc\)](#)

[Xbox Games Download](#)

[PC games \(disc\)](#)

[Windows digital games](#)

[Windows phone games](#)

[Movies & TV](#)

[Music](#)

[Deals](#)

[Sale](#)

[Microsoft Surface deals](#)

[PC deals](#)

[Xbox deals](#)

[More](#)

[Business](#)

Students & educators
Developer
Gift cards
Products
Software & services
Windows
Office
Free downloads & security
Internet Explorer
Microsoft Edge
Skype
OneNote
OneDrive
Microsoft Health
MSN
Bing
Microsoft Groove
Microsoft Movies & TV
Devices & Xbox
All Microsoft devices
Microsoft Surface
All Windows PCs & tablets
PC accessories
Xbox & games
Microsoft Lumia
All Windows phones
Microsoft HoloLens
For business
Cloud Platform
Microsoft Azure
Microsoft Dynamics 365
Windows for business
Office for business
Skype for business
Surface for business
Enterprise solutions
Small business solutions
Find a solutions provider

[Volume licensing](#)

[For developers & IT pros](#)

[Develop Windows apps](#)

[Microsoft Azure](#)

[MSDN](#)

[TechNet](#)

[Visual Studio](#)

[For students & educators](#)

[Office for students](#)

[OneNote in classroom](#)

[Shop PCs & tablets perfect for students](#)

[Microsoft in Education](#)

[Support](#)



[items in cart0](#)

Search Microsoft Search

[items in cart0](#)

[Microsoft Services Agreement](#)[Microsoft Services Agreement](#)

[FAQ](#)

[Microsoft Services Agreement](#)

[Microsoft Privacy Statement](#)

[Bing Suppliers Page](#)

[FAQ](#)

[Microsoft Services Agreement](#)

[Microsoft Privacy Statement](#)

[Bing Suppliers Page](#)

Published: **July 15, 2016** [What's new?](#)

Effective: **September 15, 2016**



[Print](#)

Microsoft Services Agreement

IF YOU LIVE IN (OR YOUR PRINCIPAL PLACE OF BUSINESS IS IN) THE UNITED STATES, PLEASE READ THE BINDING ARBITRATION CLAUSE AND CLASS ACTION WAIVER IN SECTION 15. IT AFFECTS HOW DISPUTES ARE RESOLVED.

These terms ("**Terms**") cover the use of those Microsoft's consumer products, websites, and services listed [here](#) (the "**Services**"). Many of these products previously had separate terms that were called different names, such as "Xbox Live Terms of Use" or "Skype Terms of Use," and these Terms replace those separate terms. You accept these Terms by creating a Microsoft account or Skype account, through your use of the Services, or by continuing to use the Services after being notified of a change to these Terms.

Your Privacy

Your Privacy

Your Content

Code of Conduct

Using the Services &
Support

Using Third-Party
Apps and Services

Service Availability

Updates to the
Services or Software,
and Changes to
These Terms

Software License

Payment Terms

Contracting Entity,
Choice of Law,
Jurisdiction

Warranties

Limitation of Liability

Service-Specific
Terms

1. **Your Privacy.** Your privacy is important to us. Please read the [Microsoft Privacy Statement](#) (the "**Privacy Statement**") as it describes the types of data we collect from you and your devices ("**Data**") and how we use your Data. The Privacy Statement also describes how Microsoft uses your content, which is your communications with others; postings or feedback submitted by you to Microsoft via the Services; and the files, photos, documents, audio, digital works, and videos that you upload, store or share through the Services ("**Your Content**"). By using the Services or agreeing to these Terms, you consent to Microsoft's collection, use and disclosure of Your Content and Data as described in the Privacy Statement.

Your Content

2. **Your Content.** Many of our Services allow you to store or share Your Content or receive material from others. We don't claim ownership of Your Content. Your Content remains Your Content and you are responsible for it.

a. When you share Your Content with other people, you understand that they may be able to, on a worldwide basis, use, save, record, reproduce, transmit, display (and on HealthVault delete) Your Content without compensating you. If you do not want others to have that ability, do not use the Services to share Your Content. You represent and warrant that for the duration of these Terms, you have (and will have) all the rights necessary for Your Content that is uploaded, stored, or shared on or through the Services and that the collection, use, and retention of Your Content will not violate any law or rights of others. Microsoft cannot be held responsible for Your Content or the material others upload, store or share using the Services.

b. To the extent necessary to provide the Services to you and others, to protect you and the Services, and to improve Microsoft products and services, you grant to Microsoft a worldwide and royalty-free intellectual property license to use Your Content, for example, to make copies of, retain, transmit, reformat, display, and distribute via communication tools Your Content on the Services. If you publish Your Content in areas of the Service where it is available broadly online without restrictions, Your Content may appear in demonstrations or materials that promote

Xbox Live and
Microsoft Studios
Games and
Applications

the Service. Some of the Services are supported by advertising. Controls for how Microsoft personalizes advertising are available on the [Security & privacy page](#) of the Microsoft account management website. We do not use what you say in email, chat, video calls or voice mail, or your documents, photos or other personal files to target advertising to you. Our advertising policies are covered in detail in the Privacy Statement.

Store

[↑Top of page](#)

Microsoft Family
Features

Code of Conduct

Group Messaging

Skype and GroupMe

Bing and MSN

Cortana

Outlook.com

Office-based
Services

Microsoft Health
Services

Digital Goods

OneDrive

Binding Arbitration
and Class Action
Waiver

Miscellaneous

NOTICES

STANDARD
APPLICATION
LICENSE TERMS

Covered Services

3. Code of Conduct.

a. By agreeing to these Terms, you're agreeing that, when using the Services, you will follow these rules:

- i. Don't do anything illegal.
- ii. Don't engage in any activity that exploits, harms, or threatens to harm children.
- iii. Don't send spam. Spam is unwanted or unsolicited bulk email, postings, contact requests, SMS (text messages), or instant messages.
- iv. Don't publicly display or use the Services to share inappropriate Content or material (involving, for example, nudity, bestiality, pornography, graphic violence, or criminal activity).
- v. Don't engage in activity that is false or misleading (e.g., asking for money under false pretenses, impersonating someone else, manipulating the Services to increase play count, or affect rankings, ratings, or comments).
- vi. Don't circumvent any restrictions on access to or availability of the Services.
- vii. Don't engage in activity that is harmful to you, the Services, or others (e.g., transmitting viruses, stalking, posting terrorist content, communicating hate speech, or advocating violence against others).
- viii. Don't infringe upon the rights of others (e.g., unauthorized sharing of copyrighted music or other copyrighted material, resale or other distribution of Bing maps, or photographs).
- ix. Don't engage in activity that violates the privacy of others.
- x. Don't help others break these rules.

b. **Enforcement.** If you violate these Terms, we may stop providing Services to you or we may close your Microsoft account or Skype account. We may also block delivery of a communication (like email or instant message) to or from the Services in an effort to enforce these Terms or we may remove or refuse to publish Your Content for any reason. When investigating alleged violations of these Terms, Microsoft reserves the right to review Your Content in order to resolve the issue. However, we cannot monitor the entire Services and make no attempt to do so.

c. **Application to Xbox Services.** Click [here](#) for more information about how this Code of Conduct applies to Xbox Live, Games for Windows Live and Microsoft Studios games, applications, services and content provided by Microsoft.

[↑Top of page](#)

Using the Services & Support

4. Using the Services & Support.

a. **Microsoft account or Skype account.** You'll need a Microsoft account to access many of the Services. Your Microsoft account lets you sign in to products, websites and services provided by Microsoft and some Microsoft partners. To access Skype on certain platforms, you have the option of using a Skype account or a Microsoft account.

i. **Creating an Account.** You can create a Microsoft account or a Skype account by signing up online. You agree not to use any false, inaccurate or misleading information when signing up for your Microsoft account or Skype account. In some cases, a third party, like your Internet service provider, may have assigned a Microsoft account to you. If you received your Microsoft account from a third party, the third party may have additional rights over your account, like the ability to access or delete your Microsoft account. Please review any additional terms the third party provided you, as Microsoft has no responsibility regarding these additional terms. If you create a Microsoft account on behalf of an entity, such as your business or employer, you represent that you have the legal authority to bind that entity to these Terms. You cannot transfer your Microsoft account or Skype account to another user or entity. To protect your account, keep your account details and password confidential. You are responsible for all activity that occurs under your Microsoft account or Skype account.

ii. **Account Use.** You must use your Microsoft account to keep it active. This means you must sign in at least once in a five-year period to keep your Microsoft account, and associated Services, active, unless provided otherwise in an offer for a paid portion of the Services. If you don't sign in during this time, we will assume your Microsoft account is inactive and will close it for you. Please see section 4(a)(iv)(2) for the consequences of a closed Microsoft account. You must sign into your Outlook.com inbox and your OneDrive (separately) at least once in a one-year period, otherwise we will close your Outlook.com inbox and your OneDrive for you. You must sign into the Xbox Services (defined in section 14(a)(i)) at least once in a five-year period to keep the gamertag associated with your Microsoft account. If we reasonably suspect that your Microsoft account or Skype account is being used by a third party fraudulently (for example, as a result of an account compromise), Microsoft may suspend your account until you can reclaim ownership. Based on the nature of the compromise, we may be required to disable access to some or all of Your Content. If you are having trouble accessing your Microsoft account, please visit this website: <http://go.microsoft.com/fwlink/?LinkId=238656>. To manage your Skype account, you must "Sign In" at www.skype.com.

iii. **Kids and Accounts.** By using the Services, you represent that you have either reached the age of "majority" where you live or have valid parent or legal guardian consent to be bound by these Terms. If you do not know whether you

have reached the age of majority where you live, or do not understand this section, please ask your parent or legal guardian for help before you create a Microsoft account or Skype account. If you are the parent or legal guardian of a minor that creates a Microsoft account or Skype account, you accept these Terms on the minor's behalf and are responsible for all use of the Microsoft account, Skype account, or Services, including purchases, whether the minor's account is now open or created later.

iv. Closing Your Account.

1. You can cancel specific Services or close your Microsoft account or Skype account at any time and for any reason. To close your Microsoft account, please visit <http://go.microsoft.com/fwlink/p/?linkid=618278>. When you ask us to close your Microsoft account, we will put it in a suspended state for 60 days just in case you change your mind. After that 60-day period, your Microsoft account will be closed. Please see section 4 (a)(iv)(2) below for a detailed explanation as to what happens when your Microsoft account is closed. Logging back in during that 60-day period will reactivate your Microsoft account. To cancel your Skype account please submit a support request to <http://go.microsoft.com/fwlink/p/?linkid=618280>.

2. If your Services are canceled or your Microsoft account or Skype account is closed (whether by you or us), a few things happen. First, your right to use the Services stops immediately and your license to use the software related to the Services ends. Second, we'll delete Data or Your Content associated with your Microsoft account or Skype account or will otherwise disassociate it from you and your Microsoft account or Skype account (unless we are required by law to keep it). You should have a regular backup plan as Microsoft won't be able to retrieve Your Content or Data once your account is closed. Third, you may lose access to material or products you've acquired.

b. Work or School Accounts. You can sign into certain Microsoft services with a work or school email address. If you do, you agree that the owner of the domain associated with your email address may control and administer your account, and access and process your data, including the contents of your communications and files. You further agree that your use of the services may be subject to the agreements that Microsoft has with you or your organization and these terms do not apply. If you use a work or school email address to access Services covered under these Terms, you may be prompted to update the email address associated with your Microsoft account in order to continue accessing such Services.

c. Additional Equipment/Data Plans. To use many of the Services, you'll need an internet connection and/or data/cellular plan. You might also need additional equipment, like a headset, camera or microphone. You are responsible for providing all connections, plans, and/or equipment needed to use the Services and for paying the fees charged by the provider(s) of your connections, plans, and equipment. Those fees are in addition to any fees you pay us for the Services and we will not reimburse you for such fees. Check with your provider(s) to determine if there are any such fees that may apply to you.

d. **Service Notifications.** When there's something important to tell you about a Service you use, we'll send you Service notifications to the email associated with your Microsoft account or, for Skype notifications, your Skype account. If you gave us your phone number in connection with your Microsoft account or Skype account, then we may send Service notifications to you via SMS (text message), including to verify your identity before registering your mobile phone number. **Data or messaging rates may apply when receiving notifications via SMS.**

e. **Support.** Customer support for the Services is available at <http://support.microsoft.com>.

[↑Top of page](#)

Using Third-Party Apps and Services

5. **Using Third-Party Apps and Services.** The Services may allow you to access or acquire products, services, websites, links, content, material, games or applications from third parties (companies or people who aren't Microsoft) ("**Third-Party Apps and Services**"). Many of our Services also help you find Third-Party Apps and Services, and you understand that you are directing our Services to provide Third-Party Apps and Services to you. The Third-Party Apps and Services may also allow you to store Your Content or Data with the publisher, provider, or operator of the Third-Party Apps and Services. The Third-Party Apps and Services may present you with a privacy policy or require you to accept additional terms of use before you can install or use the Third-Party App or Service. See section 14(b) for additional terms for applications acquired through the Office Store, the Xbox Store or the Windows Store. You should review any additional terms and privacy policies before acquiring or using any Third-Party Apps and Services. Any additional terms do not modify any of these Terms. You are responsible for your dealings with third parties. Microsoft does not license any intellectual property to you as part of any Third-Party Apps and Services and is not responsible for information provided by third parties.

[↑Top of page](#)

Service Availability

6. Service Availability.

a. The Services, Third-Party Apps and Services, or material or products offered through the Services may be unavailable from time to time, may be offered for a limited time, or may vary depending on your region or device. If you change the location associated with your Microsoft account, you may need to re-acquire the material or applications that were available to you and paid for in your previous region.

b. We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you've stored. We recommend that you regularly backup Your Content that you store on the Services or store using Third-Party Apps and Services.

[↑Top of page](#)

Updates to the Services or Software, and Changes to These Terms

7. Updates to the Services or Software, and Changes to These Terms.

a. We may change these Terms at any time, and we'll tell you when we do. Using the Services after the changes become effective means you agree to the new terms. If you don't agree to the new terms, you must stop using the Services, close your Microsoft account and/or Skype account and, if you are a parent or guardian, help your minor child close his or her Microsoft account or Skype account.

b. Sometimes you'll need software updates to keep using the Services. We may automatically check your version of the software and download software updates or configuration changes. You may also be required to update the software to continue using the Services. Such updates are subject to these Terms unless other terms accompany the updates, in which case, those other terms apply. Microsoft isn't obligated to make any updates available and we don't guarantee that we will support the version of the system for which you licensed the software.

c. Additionally, there may be times when we need to remove or change features or functionality of the Service or stop providing a Service or access to Third-Party Apps and Services altogether. Except to the extent required by applicable law, we have no obligation to provide a re-download or replacement of any material, Digital Goods (defined in section 14(k)), or applications previously purchased. We may release the Services or their features in a beta version, which may not work correctly or in the same way the final version may work.

d. So that you can use material protected with digital rights management (DRM), like some music, games, movies and more, DRM software may automatically contact an online rights server and download and install DRM updates.

[↑Top of page](#)

Software License

8. **Software License.** Unless accompanied by a separate Microsoft license agreement (for example, if you are using a Microsoft application that is included with and a part of

Windows, then the Microsoft Software License Terms for the Windows Operating System govern such software), and except as provided in section 14(b)(i) below for applications available through the Office Store, the Windows Store or the Xbox Store, any software provided by us to you as part of the Services is subject to these Terms.

a. If you comply with these Terms, we grant you the right to install and use one copy of the software per device on a worldwide basis for use by only one person at a time as part of your use of the Services. The software or website that is part of the Services may include third-party code. Any third-party scripts or code, linked to or referenced from the software or website, are licensed to you by the third parties that own such code, not by Microsoft. Notices, if any, for the third-party code are included for your information only.

b. The software is licensed, not sold, and Microsoft reserves all rights to the software not expressly granted by Microsoft, whether by implication, estoppel, or otherwise. This license does not give you any right to, and you may not:

- i. circumvent or bypass any technological protection measures in or relating to the software or Services;
- ii. disassemble, decompile, decrypt, hack, emulate, exploit, or reverse engineer any software or other aspect of the Services that is included in or accessible through the Services, except and only to the extent that the applicable copyright law expressly permits doing so;
- iii. separate components of the software or Services for use on different devices;
- iv. publish, copy, rent, lease, sell, export, import, distribute, or lend the software or the Services, unless Microsoft expressly authorizes you to do so;
- v. transfer the software, any software licenses, or any rights to access or use the Services;
- vi. use the Services in any unauthorized way that could interfere with anyone else's use of them or gain access to any service, data, account, or network;
- vii. enable access to the Services or modify any Microsoft-authorized device (e.g., Xbox One, Xbox 360, Microsoft Surface, etc.) by unauthorized third-party applications.

[↑Top of page](#)

Payment Terms

9. Payment Terms. If you purchase a Service, then these payment terms apply to your purchase and you agree to them.

a. **Charges.** If there is a charge associated with a portion of the Services, you agree to pay that charge. The price stated for the Services excludes all applicable taxes and currency exchange settlements, unless stated otherwise. The price for Skype paid products includes a charge for the product and a charge for taxes. You are solely responsible for paying such taxes or other charges. Taxes are calculated based on your location at the time your Microsoft or Skype account was registered. We may suspend or cancel the Services if we do not receive an on time, full payment from you. Suspension or cancellation of the Services for non-payment could result in a

loss of access to and use of your account and its content. Connecting to the Internet via a corporate or other private network which masks your location may cause charges to be different from those displayed for your actual location.

b. **Your Billing Account.** To pay the charges for a Service, you will be asked to provide a payment method at the time you sign up for that Service. You can access and change your billing information and payment method on the [Microsoft account management website](#) and for your Skype billing account by signing into your account at [www.skype.com](#). Additionally, you agree to permit Microsoft to use any updated account information regarding your selected payment method provided by your issuing bank or the applicable payment network. You agree to promptly update your account and other information, including your email address and payment method details, so we can complete your transactions and contact you as needed in connection with your transactions. Changes made to your billing account will not affect charges we submit to your billing account before we could reasonably act on your changes to your billing account.

c. **Billing.** By providing Microsoft with a payment method, you (i) represent that you are authorized to use the payment method that you provided and that any payment information you provide is true and accurate; (ii) authorize Microsoft to charge you for the Services or available content using your payment method; and (iii) authorize Microsoft to charge you for any paid feature of the Services that you choose to sign up for or use while these Terms are in force. We may bill you (a) in advance; (b) at the time of purchase; (c) shortly after purchase; or (d) on a recurring basis for subscription Services. Also, we may charge you up to the amount you have approved, and we will notify you in advance of any change in the amount to be charged for recurring subscription Services. We may bill you at the same time for more than one of your prior billing periods for amounts that haven't previously been processed.

d. **Recurring Payments.** When you purchase the Services on a subscription basis (e.g., monthly, every 3 months or annually (as applicable)), you acknowledge and agree that you are authorizing recurring payment, and payments shall be made to Microsoft by the method you have chosen at the recurring intervals chosen by you, until the subscription for that Service is terminated by you or by Microsoft. By authorizing recurring payments, you are authorizing Microsoft to process such payments as either electronic debits or fund transfers, or as electronic drafts from your designated account (in the case of Automated Clearing House or similar payments), or as charges to your designated account (in the case of credit card or similar payments) (collectively, "**Electronic Payments**"). Subscription fees are generally billed or charged in advance of the applicable subscription period. If any payment is returned unpaid or if any credit card or similar transaction is rejected or denied, Microsoft or its service providers reserve the right to collect any applicable return item, rejection or insufficient funds fee and to process any such payment as an Electronic Payment.

e. **Automatic Renewal.** Provided that automatic renewals are allowed in your state, you may choose for Services to automatically renew at the end of a fixed service period. We will remind you by email before any Services renew for a new term, and notify you of any price changes in accordance with section 9(k). Once we have

reminded you that you elected to automatically renew the Services, we may automatically renew your Services at the end of the current service period and charge you the then current price for the renewal term, unless you have chosen to cancel the Services as described below. We will also remind you that we will bill your chosen payment method for the Services renewal, whether it was on file on the renewal date or provided later. We will also provide you with instructions on how you may cancel the Services. You must cancel the Services before the renewal date to avoid being billed for the renewal.

f. **Online Statement and Errors.** Microsoft will provide you with an online billing statement on the [Microsoft account management website](#), where you can view and print your statement. For Skype accounts you can access your online statement by signing into your account at www.skype.com. This is the only billing statement that we provide. If we make an error on your bill, you must tell us within 90 days after the error first appears on your bill. We will then promptly investigate the charge. If you do not tell us within that time, you release us from all liability and claims of loss resulting from the error and we won't be required to correct the error or provide a refund. If Microsoft has identified a billing error, we will correct that error within 90 days.

g. **Refund Policy.** Unless otherwise provided by law or by a particular Service offer, all purchases are final and non-refundable. If you believe that Microsoft has charged you in error, you must contact us within 90 days of such charge. No refunds will be given for any charges more than 90 days old. We reserve the right to issue refunds or credits at our sole discretion. If we issue a refund or credit, we are under no obligation to issue the same or similar refund in the future. This refund policy does not affect any statutory rights that may apply. For more refund information, please visit our [help topic](#).

h. **Canceling the Services.** You may cancel a Service at any time, with or without cause. To cancel a Service and request a refund, if you are entitled to one, visit the [Microsoft account management website](#). You can request a refund from Skype using the [Cancellation and Refund form](#). You should refer back to the offer describing the Services as (i) you may not receive a refund at the time of cancellation; (ii) you may be obligated to pay cancellation charges; (iii) you may be obligated to pay all charges made to your billing account for the Services before the date of cancellation; or (iv) you may lose access to and use of your account when you cancel the Services. If you cancel, your access to the Services ends at the end of your current Service period or, if we bill your account on a periodic basis, at the end of the period in which you canceled.

i. **Trial-Period Offers.** If you are taking part in any trial-period offer, you must cancel the trial Service(s) by the end of the trial period to avoid incurring new charges, unless we notify you otherwise. If you do not cancel the trial Service(s) by the end of the trial period, we may charge you for the Service(s).

j. **Promotional Offers.** From time to time, Microsoft may offer Services for a trial period during which Microsoft will not charge you for the Services. Microsoft reserves the right to charge you for such Services (at the normal rate) in the event

that Microsoft determines (in its reasonable discretion) that you are breaching the terms and conditions of the offer.

k. **Price Changes.** We may change the price of the Services at any time and if you have a recurring purchase, we will notify you by email at least 15 days before the price change. If you do not agree to the price change, you must cancel and stop using the Services before the price change takes effect. If there is a fixed term and price for your Service offer, that price will remain in force for the fixed term.

l. **Payments to You.** If we owe you a payment, then you agree to timely and accurately provide us with any information we need to get that payment to you. You are responsible for any taxes and charges you may incur as a result of this payment to you. You must also comply with any other conditions we place on your right to any payment. If you receive a payment in error, we may reverse or require return of the payment. You agree to cooperate with us in our efforts to do this. We may also reduce the payment to you without notice to adjust for any previous overpayment.

m. **Gift Cards.** Redemption and use of gift cards (other than Skype gift cards) are governed by the [Microsoft Gift Card Terms and Conditions](#). Information on Skype gift cards is available on [Skype's Help page](#).

[↑Top of page](#)

Contracting Entity, Choice of Law, Jurisdiction

10. **Contracting Entity.** For use of free, consumer Skype-branded Services, you're contracting with, and all references to "Microsoft" in these Terms mean, Skype Software S.à.r.l, 23 – 29 Rives de Clausen, L-2165 Luxembourg, and for paid, consumer Skype-branded Services, you're contracting with, and all references to "Microsoft" in these Terms mean, Skype Communications S.à.r.l, 23 – 29 Rives de Clausen, L-2165 Luxembourg. For all other Services, you're contracting with Microsoft Corporation, One Microsoft Way, Redmond, WA 98052, U.S.A.

11. **Choice of Law and Place to Resolve Disputes.** If you live in (or, if a business, your principal place of business is in) the United States, the laws of the state where you live govern all claims, regardless of conflict of laws principles, except that the Federal Arbitration Act governs all provisions relating to arbitration. You and we irrevocably consent to the exclusive jurisdiction and venue of the state or federal courts in King County, Washington, for all disputes arising out of or relating to these Terms or the Services that are heard in court (excluding arbitration and small claims court).

[↑Top of page](#)

Warranties

12. **Warranties.** MICROSOFT, AND OUR AFFILIATES, RESELLERS, DISTRIBUTORS, AND VENDORS, MAKE NO WARRANTIES, EXPRESS OR IMPLIED, GUARANTEES OR CONDITIONS WITH RESPECT TO YOUR USE OF THE SERVICES. YOU UNDERSTAND THAT USE OF THE SERVICES IS AT YOUR OWN RISK AND THAT WE PROVIDE THE SERVICES ON AN "AS IS" BASIS "WITH ALL FAULTS" AND "AS AVAILABLE." YOU BEAR THE ENTIRE RISK OF USING THE SERVICES. MICROSOFT DOESN'T GUARANTEE THE ACCURACY OR TIMELINESS OF INFORMATION AVAILABLE FROM THE SERVICES. TO THE EXTENT PERMITTED UNDER YOUR LOCAL LAW, WE EXCLUDE ANY IMPLIED WARRANTIES, INCLUDING FOR MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, WORKMANLIKE EFFORT, AND NON-INFRINGEMENT. YOU MAY HAVE CERTAIN RIGHTS UNDER YOUR LOCAL LAW. NOTHING IN THESE TERMS IS INTENDED TO AFFECT THOSE RIGHTS, IF THEY ARE APPLICABLE. YOU ACKNOWLEDGE THAT COMPUTER AND TELECOMMUNICATIONS SYSTEMS ARE NOT FAULT-FREE AND OCCASIONAL PERIODS OF DOWNTIME OCCUR. WE DO NOT GUARANTEE THE SERVICES WILL BE UNINTERRUPTED, TIMELY, SECURE, OR ERROR-FREE OR THAT CONTENT LOSS WON'T OCCUR, NOR DO WE GUARANTEE ANY CONNECTION TO OR TRANSMISSION FROM THE COMPUTER NETWORKS.

[↑Top of page](#)

Limitation of Liability

13. **Limitation of Liability.** If you have any basis for recovering damages (including breach of these Terms), you agree that your exclusive remedy is to recover, from Microsoft or any affiliates, resellers, distributors, Third-Party Apps and Services providers, and vendors, direct damages up to an amount equal to your Services fee for the month during which the breach occurred (or up to \$10.00 if the Services are free). You can't recover any other damages or losses, including direct, consequential, lost profits, special, indirect, incidental, or punitive. These limitations and exclusions apply even if this remedy doesn't fully compensate you for any losses or fails of its essential purpose or if we knew or should have known about the possibility of the damages. To the maximum extent permitted by law, these limitations and exclusions apply to anything or any claims related to these Terms, the Services, or the software related to the Services.

[↑Top of page](#)

Service-Specific Terms

14. **Service-Specific Terms.** The terms before and after section 14 apply generally to all Services. This section contains service-specific terms that are in addition to the general terms.

[↑Top of page](#)

Xbox Live and Microsoft Studios Games and Applications

a. Xbox Live and Microsoft Studios Games and Applications.

i. **Personal Noncommercial Use.** Xbox Live, Games for Windows Live and Microsoft Studios games, applications, services and content provided by Microsoft (collectively, the "**Xbox Services**") are only for your personal and noncommercial use.

ii. **Sharing Limited Account Information.** As part of delivering the Xbox Services, we make information pertaining to your gamertag, gameplay, Your Content that you make public, and activity on and usage of any Xbox Service available for the operation and delivery of (a) other Xbox Services and (b) third-party games that use Xbox Services. If you choose to link your Microsoft Xbox Services account with your account on a non-Microsoft service (for example, a non-Microsoft game publisher of Third-Party Apps and Services), you agree that: (a) Microsoft may share limited account information (including without limitation gamertag, gamerscore, game score, game history, and friends list), with that non-Microsoft party as stated in the Microsoft Privacy Statement, and (b) if allowed by your Xbox privacy settings, the non-Microsoft party may also have access to Your Content from in-game communications when you are signed into your account with that non-Microsoft party. Also, if allowed by your Xbox privacy settings, Microsoft can publish your name, gamertag, gamerpics, motto, avatar, and games that you've played in communications to people on your Xbox friends list.

iii. **Your Content.** As part of building the Xbox Services community, you grant to Microsoft, its affiliates and sublicensees a free and worldwide right to use, modify, reproduce, distribute, and display Your Content or your name, gamertag, motto, or avatar that you posted for any Xbox Services.

iv. **Game Managers.** Some games may use game managers and hosts. Game managers and hosts are not authorized Microsoft spokespersons. Their views do not necessarily reflect those of Microsoft.

v. **Kids on Xbox.** If you are a minor using Xbox Live, your parent or guardian may have control over many aspects of your account and may receive reports about your use of Xbox Live.

vi. **Game Currency or Virtual Goods.** The Services may include a virtual, game currency (like gold, coins or points) that may be purchased from Microsoft using actual monetary instruments if you have reached the age of "majority" where you live. The Services may also include virtual, digital items or goods that may be purchased from Microsoft using actual monetary instruments or using game currency. Game currency and virtual goods may never be redeemed for actual monetary instruments, goods or other items of monetary value from Microsoft or any other party. Other than a limited, personal, revocable, non-transferable, non-sublicensable license to use the game currency and virtual

goods in the Services only, you have no right or title in or to any such game currency or virtual goods appearing or originating in the Services, or any other attributes associated with use of the Services or stored within the Services. Microsoft may at any time regulate, control, modify and/or eliminate the game currency and/or virtual goods as it sees fit in its sole discretion.

vii. **Software Updates.** For any device that can connect to Xbox Services, we may automatically check your version of Xbox console software or the Xbox App software and download Xbox console or Xbox App software updates or configuration changes, including those that prevent you from accessing the Xbox Services, using unauthorized Xbox games or Xbox apps, or using unauthorized hardware peripheral devices with an Xbox console.

viii. **Gamertag Expiration.** You must sign into Xbox Services at least once in a five-year period, otherwise you may lose access to the gamertag associated with your account and that gamertag may become available for use by others.

[↑Top of page](#)

Store

b. **Store.** "Store" refers to a Service that allows you to browse, download, purchase, and rate and review applications (the term "application" includes games) and other digital content. These Terms cover use of Office Store, Xbox Store and Windows Store. "**Office Store**" means a Store for Office products and apps for Office, SharePoint, Exchange, Access and Project (2013 versions or later). "**Windows Store**" means a Store for Windows devices such as phone, PC and tablet, or any other experience that is branded Windows Store. "**Xbox Store**" means a Store for Xbox ONE and Xbox 360 consoles, or any other experience that is branded Xbox Store.

i. **License Terms.** We will identify the publisher of each application available in the relevant Store. The Standard Application License Terms ("**SALT**") at the end of these Terms are an agreement between you and the application publisher setting forth the license terms that apply to your use of an application you download through the Windows Store or the Xbox Store, unless different license terms are provided with the application. Section 5 of these Terms applies to any Third-Party Apps and Services acquired through a Store. Applications downloaded through the Office Store are not governed by the SALT and have separate license terms that apply.

ii. **Updates.** Microsoft will automatically check for and download updates to your applications, even if you're not signed into the relevant Store. You can change your Store or system settings if you prefer not to receive automatic updates to Store applications. However, certain Office Store applications that are entirely or partly hosted online may be updated at any time by the application developer and may not require your permission to update.

iii. **Ratings and Reviews.** If you rate or review an application in the Store, you may receive email from Microsoft containing content from the publisher of the application. Any such email comes from Microsoft; we do not share your email address with publishers of applications you acquire through the Store.

iv. **Safety Warning.** To avoid possible injury, discomfort or eye strain, you should take periodic breaks from use of games or other applications, especially if you feel any pain or fatigue resulting from usage. If you experience discomfort, take a break. Discomfort might include feelings of nausea, motion sickness, dizziness, disorientation, headache, fatigue, eye strain, or dry eyes. Using applications can distract you and obstruct your surroundings. Avoid trip hazards, stairs, low ceilings, fragile or valuable items that could be damaged. A very small percentage of people may experience seizures when exposed to certain visual images like flashing lights or patterns that may appear in applications. Even people with no history of seizures may have an undiagnosed condition that can cause these seizures. Symptoms may include lightheadedness, altered vision, twitching, jerking or shaking of limbs, disorientation, confusion, loss of consciousness, or convulsions. Immediately stop using and consult a doctor if you experience any of these symptoms, or consult a doctor before using the applications if you've ever suffered symptoms linked to seizures. Parents should monitor their children's use of applications for signs of symptoms.

[↑Top of page](#)

Microsoft Family Features

c. **Microsoft Family Features.** Parents and kids can use Microsoft family features to build trust based on a shared understanding of what behaviors, websites, apps, games, physical locations, and spending is right in their family. Parents can create a family by going to <https://account.microsoft.com/family> (or by following the instructions on their Windows device or Xbox console) and inviting kids or other parents to join. There are many features available to family members, so please carefully review the information provided when you agree to create or join a family. By creating or joining a family, you represent that you will use the family in accordance with its purpose and won't use it in an unauthorized way to unlawfully gain access to another person's information.

[↑Top of page](#)

Group Messaging

d. **Group Messaging.** Various Microsoft services allow you to send messages to others via voice or SMS ("messages"), and/or allow Microsoft and Microsoft-

controlled affiliates to send such messages to you and one or more other users on your behalf. WHEN YOU INSTRUCT MICROSOFT AND MICROSOFT-CONTROLLED AFFILIATES TO SEND SUCH MESSAGES TO YOU OR TO OTHERS, YOU REPRESENT AND WARRANT TO US THAT YOU AND EACH PERSON YOU HAVE INSTRUCTED US TO MESSAGE CONSENT TO RECEIVE SUCH MESSAGES AND ANY OTHER RELATED ADMINISTRATIVE TEXT MESSAGES FROM MICROSOFT AND MICROSOFT-CONTROLLED AFFILIATES. "Administrative text messages" are periodic transactional messages from a particular Microsoft service, including but not limited to a "welcome message" or instructions on how to stop receiving messages. You or group members no longer wishing to receive such messages can opt-out of receiving further messages from Microsoft or Microsoft-controlled affiliates at any time by following the instructions provided. If you no longer wish to receive such messages or participate in the group, you agree that you will opt out through the instructions provided by the applicable program or service. If you have reason to believe that a group member no longer wishes to receive such messages or participate in the group, you agree to remove them from the group. You also represent and warrant to us that you and each person you have instructed us to message understands that each group member is responsible for the costs of any message charges assessed by his or her mobile carrier, including any international message charges that may apply when messages are transmitted from US-based numbers.

[↑Top of page](#)

Skype and GroupMe

e. Skype and GroupMe.

i. **No Access to Emergency Services.** There are important differences between traditional telephone services and Skype. Skype is not required to offer access to Emergency Services under any applicable local and/or national rules, regulations, or law. Skype's software and products are not intended to support or carry emergency calls to any type of hospitals, law enforcement agencies, medical care units or any other kind of services that connect a user to emergency services personnel or public safety answering points ("**Emergency Services**"). You acknowledge and agree that: (i) it is your responsibility to purchase traditional wireless (mobile) or fixed-line telephone services that offer access to Emergency Services, and (ii) Skype is not a replacement for your primary telephone service.

ii. **APIs or Broadcasting.** If you want to use Skype in connection with any broadcast, you must comply with the "Broadcast TOS" at <http://www.skype.com/legal/broadcast>. If you want to use any application program interface ("**API**") exposed or made available by Skype you must comply with the applicable licensing terms, which are available at www.skype.com/go/legal.

iii. **Fair Use Policies.** Fair usage policies may apply to your use of Skype. Please review these policies which are designed to protect against fraud and abuse and may place limits on the type, duration or volume of calls or messages that you are able to make. These policies are incorporated in these Terms by reference. You can find these policies at: <http://www.skype.com/en/legal/fair-usage/>

iv. **Mapping.** Skype contains features that allow you to submit information to, or plot yourself on a map using, a mapping service. By using those features, you agree to these Terms and the Google Maps terms available at http://www.google.com/intl/en_ALL/help/terms_maps.html.

v. **Government Users.** If you wish to use a business account and/or Skype Manager on behalf of the U.S. Government or an agency of the U.S. Government, these Terms do not apply to that use. For applicable terms and/or further information, please contact usgovusers@skype.net.

vi. **Personal/Noncommercial Use.** The use of Skype is for your personal and noncommercial use. You are permitted to use your personal Skype account at work for your own business communications.

vii. **Skype Number/Skype To Go.** If Skype provides you with a Skype Number or Skype To Go number, you agree that you do not own the number or have a right to retain that number forever.

viii. **Skype Manager.** A "Skype Manager Admin Account" is a Skype account that is created and managed by you, acting as an individual administrator of a Skype Manager group and not as a business entity. Personal Skype accounts can be linked to a Skype Manager group ("**Linked Account**"). You may appoint additional administrators to your Skype Manager group subject to their acceptance of these Terms. If you allocate Skype Numbers to a Linked Account, you are responsible for compliance with any requirements related to the residency or location of your Linked Account users. If you choose to unlink a Linked Account from a Skype Manager group, any allocated subscriptions, Skype Credit or Skype Numbers will not be retrievable and Your Content or material associated with the unlinked Skype account will no longer be accessible by you. You agree to process any personal information of your Linked Account users in accordance with all applicable data protection laws.

ix. **Skype Charges.** Skype paid products are sold to you by Skype Communications S.à.r.l, however the seller-of-record accountable for taxes is Skype Communications US Corporation. Taxes means the amount of taxes, regulatory fees, surcharges or other fees that we are required to collect from you and must pay to any United States (federal, state or local) or foreign government, agency, commission or quasi-governmental body as a result of our provision of Skype paid products to you. These taxes are listed at www.skype.com/go/ustax. All prices for Skype paid products are inclusive of a charge for your product and a charge for taxes, unless otherwise stated. The charges payable for calling phones outside of a subscription consist of a connection fee (charged once per call) and a per-minute rate as set out at www.skype.com/go/allrates. Call charges will be deducted from your Skype

Credit balance. Skype may change its calling rates at any time without notice to you by posting such change at www.skype.com/go/allrates. The new rate will apply to your next call after publication of the new rates. Please check the latest rates before you make your call. Fractional call minutes and fractional cent charges will be rounded up to the next whole unit.

x. **Skype Credit.** Skype does not guarantee that you will be able to use your Skype Credit balance to purchase all Skype paid products. If you do not use your Skype Credit for a period of 180 days, Skype will place your Skype Credit on inactive status. You can reactivate the Skype Credit by following the reactivation link at <http://www.skype.com/go/store.reactivate.credit>. You can enable the Auto Recharge feature when you buy Skype Credit by ticking the appropriate box. If enabled, your Skype Credit balance will be recharged with the same amount and by your chosen payment method every time your Skype account balance goes below the threshold set by Skype from time to time. If you purchased a subscription with a payment method other than credit card, PayPal or Moneybookers (Skrill), and you have enabled Auto-Recharge, your Skype Credit balance will be recharged with the amount necessary to purchase your next recurring subscription. You can disable Auto-Recharge at any time by accessing and changing your settings in your Skype account.

xi. **International Message Fees.** GroupMe currently uses US-based numbers for each group created. Every text message sent to or received from a GroupMe number will count as an international text message sent to or received from the United States. Please check with your provider for the associated international rates.

[↑Top of page](#)

Bing and MSN

f. Bing and MSN.

i. **Bing and MSN Materials.** The articles, text, photos, maps, videos, video players, and third-party material available on Bing and MSN are for your noncommercial, personal use only. Other uses, including downloading, copying, or redistributing these materials, are permitted only to the extent specifically authorized by Microsoft or rights holders, or allowed by applicable copyright law. Microsoft or other rights holders reserve all rights to the material not expressly granted by Microsoft under the license terms, whether by implication, estoppel, or otherwise.

ii. **Bing Maps.** You may not use Bird's eye imagery of the United States, Canada, Mexico, New Zealand, Australia or Japan for governmental use without our separate written approval.

iii. **Rewards.** Rewards (the "Program") enables you to earn redeemable points for your qualified searches, acquisitions, and other offers from Microsoft. A search is the act of an individual user manually entering text for the good faith

purpose of obtaining Bing search results for such user's own research purposes and does not include any query entered by a bot, macro, or other automated or fraudulent means of any kind ("**Search**"). An acquisition is the process of purchasing goods or downloading and acquiring a license for digital content from Microsoft, whether free or paid ("**Acquisition**"). Microsoft in its sole discretion determines what constitutes a Search or Acquisition that qualifies for points. Your earned points can be redeemed for items ("**Rewards**") in the [redemption center](#). For more information see the [Frequently Asked Questions](#) ("**FAQ**").

1. *Program Requirements.* You need a valid Microsoft account and your devices must meet the [minimum system requirements](#). The Program is open to users who reside in the markets listed in the [FAQ](#). Individuals can have no more than one Program account, even if an individual has multiple email addresses, and households are limited to six accounts. The Program is solely for your personal and noncommercial use.

2. *Points.* Except for donating your points to a nonprofit organization listed in the redemption center, you cannot transfer points. Points are not your personal property, and you may not obtain any cash or money in exchange for them. Points are awarded to you on a promotional basis. You cannot purchase points. Microsoft may limit the quantity of points or Rewards per person, per household, or over a set period (e.g., a day). You may redeem no more than 550,000 points per calendar year in the Program. Points earned in the Program are not valid in, and may not be used in combination with, any other program offered by Microsoft or third parties. **Unredeemed points expire if you do not earn or redeem any points for 90 days.**

3. *Rewards.* You may redeem your points by visiting the [redemption center](#) or you may contribute points to a listed nonprofit organization. There may be a limited number of a particular Reward available, and those Rewards will be delivered on a first-come, first-served basis. You may be required to provide additional information, like your mailing address and a telephone number (other than a VOIP or toll-free number), and you may also be asked to enter a fraud-prevention code or sign additional legal documents to redeem points for Rewards. Once you order a Reward, you cannot cancel it or return it for a refund of points. If you order a Reward that is out of stock or unavailable for other reasons Microsoft determines in its sole discretion, we may substitute a Reward of comparable value or refund your points. Microsoft may update the Rewards offered in the redemption center or discontinue to offer specific Rewards. Some Rewards may have age eligibility requirements. You are responsible for all federal, state, and local taxes and any other costs of accepting and using the Reward. Rewards will be emailed to the email address you provide when ordering your Reward, so keep your email address up to date. Rewards that are undeliverable will not be reissued and are therefore forfeited. Rewards are not for resale.

4. *Cancelling Your Participation in the Program.* Your Program account will be cancelled if you do not log in at least once in a 180-day period. Additionally, Microsoft reserves the right to cancel the Program account of a specific user without cause and without providing a reason. Upon Program cancellation (by you or us) or if the Program is suspended, you will have 90 days to redeem your points; otherwise, those points will be forfeited. At the point of cancellation, your right to use the Program and accrue future points ends.

5. *Other Conditions.* Microsoft reserves the right to disqualify you; disable your access to the Program or your Rewards account; and/or withhold points, Rewards and charitable contributions, if Microsoft believes you are tampering with or abusing any aspect of the Program or may be engaging in activities that violate these Terms.

iv. **Bing Places.** When you provide your Data or Your Content to Bing Places, you grant Microsoft a worldwide, royalty-free intellectual property license to use, reproduce, save, modify, aggregate, promote, transmit, display or distribute as part of a service, and sub-license those rights to third parties.

[↑Top of page](#)

Cortana

g. **Cortana.** Cortana is Microsoft's personal assistant Service. Cortana provides information for your planning purposes only and you should exercise your own independent judgment when reviewing and relying on this information. Microsoft does not guarantee the accuracy, completeness, reliability, availability or timeliness of inferences and personalized experiences provided by Cortana. Microsoft is not responsible if a Cortana communication management feature delays or prevents you from reviewing or sending a communication.

[↑Top of page](#)

Outlook.com

h. **Outlook.com.** The Outlook.com (or @msn, @hotmail, or @live) email address that you use to create your Microsoft account will be unique to you for as long as your Outlook.com inbox or Microsoft account is still active. In the event your Outlook.com inbox or Microsoft account is closed either by you or by Microsoft pursuant to these Terms, the email address or username may be recycled into our system and assigned to another user.

[↑Top of page](#)

Office-based Services

- i. **Office-based Services.** Office consumer-based services, applications, or products (including Sway and OneNote) are for your personal, noncommercial use, unless you have commercial use rights under a separate agreement with Microsoft.

[↑Top of page](#)

Microsoft Health Services

j. **Microsoft Health Services.**

i. **HealthVault.** HealthVault is intended for you to store your personal health-related information and information about other people (such as your family) with their consent. HealthVault accounts are not for use by healthcare providers or for any other commercial or non-personal purpose. The information in your account may not always be accurate or up-to-date and should be viewed by any health care provider as informational only. The HealthVault Service does not hold records for healthcare providers or other medical or case management purposes. For example, HealthVault records are not designated record sets as defined under U.S. regulations. If a healthcare provider decides to include any data made available from HealthVault in its records, it should store a copy in its own system. If there is a co-custodian of a record in your account (because one of you invited the other), you acknowledge that the co-custodian has full control over that record and may cancel your access to the record, manage other peoples' access to the record, and view the record's data including how and when the record is used. Microsoft does not support non-Microsoft credentials (such as Facebook and OpenID), so HealthVault customer support will not be able to help with sign-in issues for those. If you lose your sign-in credentials, or if the account where you got your credentials closes, you will not be able to recover your stored data. To help maintain continued access, we suggest you use more than one sign-in credential with your HealthVault account. Microsoft does not endorse or control, and is not responsible for, the operation, support, or security of non-Microsoft credentials you may use.

ii. **Microsoft Health and Microsoft Band.** Microsoft Health and the Microsoft Band are not medical devices and are intended for fitness and wellness purposes only. They are not designed or intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease. Before starting or modifying any activity or sleep program using Microsoft Health, consult your physician. Microsoft is not responsible for any decision you make based on information you receive from Microsoft.

[↑Top of page](#)

Digital Goods

k. **Digital Goods.** Through Microsoft Groove, Microsoft Movies & TV, Store and any other related and future services, Microsoft may enable you to obtain, listen to, view, play or read (as the case may be) music, images, video, text, books, games or other material ("**Digital Goods**") that you may get in digital form. The Digital Goods are only for your personal, noncommercial entertainment use. You agree not to redistribute, broadcast, publicly perform or publicly display or transfer any copies of the Digital Goods. Digital Goods may be owned by Microsoft or by third parties. In all circumstances, you understand and acknowledge that your rights with respect to Digital Goods are limited by these Terms, copyright law, and the usage rules located at <http://go.microsoft.com/fwlink/p/?LinkId=723143>. You agree that you will not attempt to modify any Digital Goods obtained through any of the Services for any reason whatsoever, including for the purpose of disguising or changing ownership or source of the Digital Goods. Microsoft or the owners of the Digital Goods may, from time to time, remove Digital Goods from the Services without notice.

[↑Top of page](#)

OneDrive

I. OneDrive.

i. **Storage Allocation.** If you have more content stored in your OneDrive account than is provided to you under the terms of your free or paid subscription service for OneDrive and you do not respond to notice from Microsoft to fix your account by removing excess content or moving to a new subscription plan with more storage, we reserve the right to close your account and delete or disable access to Your Content on OneDrive.

ii. **Service Performance.** Depending on factors such as your equipment, internet connection and Microsoft's efforts to maintain the performance and integrity of its service, you may occasionally experience delays in uploading or syncing content on OneDrive.

[↑Top of page](#)

Binding Arbitration and Class Action Waiver

15. **Binding Arbitration and Class Action Waiver If You Live In (or If a Business Your Principal Place of Business Is In) the United States.** We hope we never have a dispute, but if we do, you and we agree to try for 60 days to resolve it informally. If we can't, you

and we agree to **binding individual arbitration before the American Arbitration Association ("AAA") under the Federal Arbitration Act ("FAA"), and not to sue in court in front of a judge or jury.** Instead, a neutral arbitrator will decide and the arbitrator's decision will be final except for a limited right of review under the FAA. **Class action lawsuits, class-wide arbitrations, private attorney-general actions, and any other proceeding where someone acts in a representative capacity aren't allowed. Nor is combining individual proceedings without the consent of all parties.** "We," "our," and "us" includes Microsoft, Skype (see section 10) and Microsoft's affiliates and, if you use Skype Pay by Mobile, your mobile phone carrier.

a. **Disputes Covered—Everything Except IP.** The term "dispute" is as broad as it can be. It includes any claim or controversy between you and us concerning the Services, the software related to the Services, the Services' or software's price, your Microsoft account, your Skype account, or these Terms, under any legal theory including contract, warranty, tort, statute, or regulation, **except disputes relating to the enforcement or validity of your, your licensors', our, or our licensors' intellectual property rights.**

b. **Mail a Notice of Dispute First.** If you have a dispute and our customer service representatives can't resolve it, send a Notice of Dispute by U.S. Mail to **Microsoft Corporation, ATTN: CELA Arbitration, One Microsoft Way, Redmond, WA 98052-6399, U.S.A.** (or to your mobile phone carrier at its principal place of business in the United States marked ATTN: Legal Department). Tell us your name, address, how to contact you, what the problem is, and what you want. A form is available at <http://go.microsoft.com/fwlink/?LinkId=245499>. We'll do the same if we have a dispute with you. After 60 days, you or we may start an arbitration if the dispute is unresolved.

c. **Small Claims Court Option.** Instead of mailing a Notice of Dispute, you may sue us in small claims court in your county of residence (or if a business your principal place of business) or King County, Washington, U.S.A. if you meet the court's requirements.

d. **Arbitration Procedure.** The AAA will conduct any arbitration under its Commercial Arbitration Rules (or if you are an individual and use the Services for personal or household use, or if the value of the dispute is \$75,000 or less whether or not you are an individual or how you use the Services, its Consumer Arbitration Rules). For more information, see www.adr.org or call 1-800-778-7879. To start an arbitration, submit the form available at <http://go.microsoft.com/fwlink/?LinkId=245497> to the AAA and mail a copy to us. In a dispute involving \$25,000 or less, any hearing will be telephonic unless the arbitrator finds good cause to hold an in-person hearing instead. Any in-person hearing will take place in your county of residence (or if a business your principal place of business) or our principal place of business—King County, Washington if your dispute is with Microsoft. You choose. The arbitrator may award the same damages to you individually as a court could. The arbitrator may award declaratory or injunctive relief only to you individually to satisfy your individual claim.

e. **Arbitration Fees and Payments.**

i. **Disputes Involving \$75,000 or Less.** We will promptly reimburse your filing fees and pay the AAA's and arbitrator's fees and expenses. If you reject our last written settlement offer made before the arbitrator was appointed, your dispute goes all the way to an arbitrator's decision (called an "award"), and the arbitrator awards you more than this last written offer, we will: (i) pay the greater of the award or \$1,000; (ii) pay your reasonable attorney's fees, if any; and (iii) reimburse any expenses (including expert witness fees and costs) that your attorney reasonably accrues for investigating, preparing, and pursuing your claim in arbitration.

ii. **Disputes Involving More than \$75,000.** The AAA rules will govern payment of filing fees and the AAA's and arbitrator's fees and expenses.

f. **Conflict with AAA Rules.** These Terms govern to the extent they conflict with the AAA's Commercial Arbitration Rules or Consumer Arbitration Rules.

g. **Must File Within One Year.** You and we must file in small claims court or arbitration any claim or dispute (except intellectual property disputes—see section 15(a)) within one year from when it first could be filed. Otherwise, it's permanently barred.

h. **Rejecting Future Arbitration Changes.** You may reject any change we make to section 15 (except address changes) by sending us notice within 30 days of the change by U.S. Mail to the address in section 15(b). If you do, the most recent version of section 15 before the change you rejected will apply.

i. **Severability.** If the class action waiver is found to be illegal or unenforceable as to all or some parts of a dispute, then those parts won't be arbitrated but will proceed in court, with the rest proceeding in arbitration. If any other provision of section 15 is found to be illegal or unenforceable, that provision will be severed but the rest of section 15 still applies.

j. **Mobile Phone Carrier as Third-Party Beneficiary.** If you use Skype Pay by Mobile, your mobile phone carrier is a third-party beneficiary of your agreement with Microsoft and Skype to resolve disputes through informal negotiation and arbitration. Your mobile phone carrier agrees to do everything Microsoft and Skype agree to do in section 15.

[↑Top of page](#)

Miscellaneous

16. **Miscellaneous.** This section, and sections 1, 9 (for amounts incurred before the end of these Terms), 10, 11, 12, 13, 15, and those that by their terms apply after the Terms end will survive any termination or cancellation of these Terms. We may assign these Terms, in whole or in part, at any time without notice to you. You may not assign your rights or obligations under these Terms or transfer any rights to use the Services. This is the entire agreement between you and Microsoft for your use of the Services. It supersedes any prior agreements between you and Microsoft regarding your use of the

Services. All parts of these Terms apply to the maximum extent permitted by relevant law. If a court or arbitrator holds that we can't enforce a part of these Terms as written, we may replace those terms with similar terms to the extent enforceable under the relevant law, but the rest of these Terms won't change. Section 15(i) says what happens if parts of section 15 (arbitration and class action waiver) are found to be illegal or unenforceable. Section 15(i) prevails over this section if inconsistent with it. Except for section 15 (arbitration and class action waiver) these Terms are solely for your and our benefit; they aren't for the benefit of any other person, except for Microsoft's successors and assigns.

17. Export Laws. You must comply with all domestic and international export laws and regulations that apply to the software and/or Services, which include restrictions on destinations, end users, and end use. For further information on geographic and export restrictions, visit <http://go.microsoft.com/fwlink/?linkid=141397> and <http://www.microsoft.com/exporting>.

18. Unsolicited Ideas. Microsoft does not consider or accept unsolicited proposals or ideas, including without limitation ideas for new products, technologies, promotions, product names, product feedback and product improvements ("**Unsolicited Feedback**"). If you send any Unsolicited Feedback to Microsoft through the Services or otherwise, you acknowledge and agree that Microsoft shall not be under any obligation of confidentiality with respect to the Unsolicited Feedback.

[↑Top of page](#)

NOTICES

Notices and procedure for making claims of intellectual property infringement. Microsoft respects the intellectual property rights of third parties. If you wish to send a notice of intellectual property infringement, including claims of copyright infringement, please use our procedures for submitting [Notices of Infringement](#). **ALL INQUIRIES NOT RELEVANT TO THIS PROCEDURE WILL NOT RECEIVE A RESPONSE.**

Microsoft uses the processes set out in Title 17, United States Code, Section 512 to respond to notices of copyright infringement. In appropriate circumstances, Microsoft may also disable or terminate accounts of users of Microsoft services who may be repeat infringers.

Notices and procedures regarding intellectual property concerns in advertising. Please review our [Intellectual Property Guidelines](#) regarding intellectual property concerns on our advertising network.

Copyright and trademark notices. The Services are copyright © 2016 Microsoft Corporation and/or its suppliers, One Microsoft Way, Redmond, WA 98052, U.S.A. All rights reserved. Microsoft and the names, logos, and icons of all Microsoft products, software, and services may be either [trademarks or registered trademarks of Microsoft](#) in the United States and/or other countries. The names of actual companies and products may be the trademarks of their respective owners. Any rights not expressly granted in these Terms are reserved. Certain software used in certain Microsoft website servers is based in part on the work of the Independent JPEG Group. Copyright © 1991-1996

Thomas G. Lane. All rights reserved. "gnuplot" software used in certain Microsoft website servers is copyright © 1986-1993 Thomas Williams, Colin Kelley. All rights reserved.

Medical notice. Microsoft does not provide medical or any other health care advice, diagnosis, or treatment. Always seek the advice of your physician or other qualified health care provider with any questions you may have regarding a medical condition, diet, fitness, or wellness program. Never disregard professional medical advice or delay in seeking it because of information you accessed on or through the Services.

Stock quotes and index data (including index values). © 2013 Morningstar, Inc. All Rights Reserved. The information contained herein: (1) is proprietary to Morningstar and/or its content providers; (2) may not be copied or distributed; and (3) is not warranted to be accurate, complete or timely. Neither Morningstar nor its content providers are responsible for any damages or losses arising from any use of this information. Past performance is no guarantee of future results.

You may not use any of the Dow Jones IndexesSM, index data, or the Dow Jones marks in connection with the issuance, creation, sponsorship, trading, marketing, or promotion of any financial instruments or investment products (for example, derivatives, structured products, investment funds, exchange-traded funds, investment portfolios, etc., where the price, return and/or performance of the instrument or investment product is based on, related to, or intended to track any of the Indexes or a proxy for any of the Indexes) without a separate written agreement with Dow Jones.

Financial notice. Microsoft isn't a broker/dealer or registered investment advisor under United States federal securities law or securities laws of other jurisdictions and doesn't advise individuals as to the advisability of investing in, purchasing, or selling securities or other financial products or services. Nothing contained in the Services is an offer or solicitation to buy or sell any security. Neither Microsoft nor its licensors of stock quotes or index data endorse or recommend any particular financial products or services. Nothing in the Services is intended to be professional advice, including but not limited to, investment or tax advice.

Notice about the H.264/AVC, MPEG-4 Visual, and VC-1 Video Standards. The software may include H.264/AVC, MPEG-4 Visual and/or VC-1 codec technology that may be licensed by MPEG LA, L.L.C. This technology is a format for data compression of video information. MPEG LA, L.L.C. requires this notice:

THIS PRODUCT IS LICENSED UNDER THE H.264/AVC, MPEG-4 VISUAL, AND THE VC-1 PATENT PORTFOLIO LICENSES FOR THE PERSONAL AND NONCOMMERCIAL USE OF A CONSUMER TO (A) ENCODE VIDEO IN COMPLIANCE WITH THE STANDARDS ("VIDEO STANDARDS") AND/OR (B) DECODE H.264/AVC, MPEG-4 VISUAL, AND VC-1 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NONCOMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE SUCH VIDEO. NONE OF THE LICENSES EXTEND TO ANY OTHER PRODUCT REGARDLESS OF WHETHER SUCH PRODUCT IS INCLUDED WITH THIS SOFTWARE IN A SINGLE ARTICLE. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE THE [MPEG LA WEBSITE](http://www.mpeg-la.com).

For clarification purposes only, this notice does not limit or inhibit the use of the software provided under these Terms for normal business uses that are personal to that business which do not include (i) redistribution of the software to third parties, or (ii)

creation of material with the VIDEO STANDARDS compliant technologies for distribution to third parties.

[↑Top of page](#)

STANDARD APPLICATION LICENSE TERMS

STANDARD APPLICATION LICENSE TERMS

WINDOWS STORE AND XBOX STORE

These license terms are an agreement between you and the application publisher. Please read them. They apply to the software applications you download from the Windows Store or the Xbox Store, including any updates or supplements for the application, unless the application comes with separate terms, in which case those terms apply.

BY DOWNLOADING OR USING THE APPLICATION, OR ATTEMPTING TO DO ANY OF THESE, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THEM, YOU HAVE NO RIGHT TO AND MUST NOT DOWNLOAD OR USE THE APPLICATION.

The application publisher means the entity licensing the application to you, as identified in the Windows Store or Xbox Store.

If you comply with these license terms, you have the rights below.

1. **INSTALLATION AND USE RIGHTS; EXPIRATION.** For applications you download from the Windows Store: (a) you may install and use the application on a Windows device or devices that are affiliated with the Microsoft account that you use to access the Windows Store; and (b) the device limit for the application is displayed in the Store or, for some applications downloaded on the Xbox console, in our [Usage Rules](#). For applications you download from the Xbox Store, you may install and use the application on Xbox consoles as described in our [Usage Rules](#). Microsoft reserves the right to modify our [Usage Rules](#) at any time.

2. **INTERNET-BASED SERVICES.**

a. **Consent for Internet-based or wireless services.** If the application connects to computer systems over the Internet, which may include via a wireless network, using the application operates as your consent to the transmission of standard device information (including but not limited to technical information about your device, system, and application software, and peripherals) for Internet-based or wireless services. If other terms are presented in connection with your use of services accessed using the application, those terms also apply.

b. **Misuse of Internet-based services.** You may not use any Internet-based service in any way that could harm it or impair anyone else's use of it or the wireless network. You may not use the service to try to gain unauthorized access to any service, data, account, or network by any means.

3. **SCOPE OF LICENSE.** The application is licensed, not sold. This agreement only gives you some rights to use the application. If Microsoft disables the ability to use

the applications on your devices pursuant to your agreement with Microsoft, any associated license rights will terminate. Application publisher reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the application only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the application that only allow you to use it in certain ways. You may not:

- a. Work around any technical limitations in the application.
- b. Reverse engineer, decompile, or disassemble the application, except and only to the extent that applicable law expressly permits, despite this limitation.
- c. Make more copies of the application than specified in this agreement or allowed by applicable law, despite this limitation.
- d. Publish or otherwise make the application available for others to copy.
- e. Rent, lease, or lend the application.
- f. Transfer the application or this agreement to any third party.

4. **DOCUMENTATION.** If documentation is provided with the application, you may copy and use the documentation for personal reference purposes.

5. **TECHNOLOGY AND EXPORT RESTRICTIONS.** The application may be subject to United States or international technology control or export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the technology used or supported by the application. These laws include restrictions on destinations, end users, and end use. For information on Microsoft branded products, go to the [Microsoft exporting website](#).

6. **SUPPORT SERVICES.** Contact the application publisher to determine if any support services are available. Microsoft, your hardware manufacturer and your wireless carrier (unless one of them is the application publisher) aren't responsible for providing support services for the application.

7. **ENTIRE AGREEMENT.** This agreement, any applicable privacy policy, any additional terms that accompany the application, and the terms for supplements and updates are the entire license agreement between you and application publisher for the application.

8. **APPLICABLE LAW.**

a. **United States and Canada.** If you acquired the application in the United States or Canada, the laws of the state or province where you live (or, if a business, where your principal place of business is located) govern the interpretation of these terms, claims for breach of them, and all other claims (including consumer protection, unfair competition, and tort claims), regardless of conflict of laws principles.

b. **Outside the United States and Canada.** If you acquired the application in any other country, the laws of that country apply.

9. **LEGAL EFFECT.** This agreement describes certain legal rights. You may have other rights under the laws of your state or country. This agreement doesn't change your rights under the laws of your state or country if the laws of your state or country don't permit it to do so.

10. **DISCLAIMER OF WARRANTY.** The application is licensed "as is," "with all faults," and "as available." You bear the entire risk as to its quality, safety, comfort, and performance. Should it prove defective, you assume the entire cost of all necessary servicing or repair. The application publisher, on behalf of itself, Microsoft, wireless carriers over whose network the application is provided, and each of our respective affiliates, vendors, agents, and suppliers ("Covered Parties"), gives no express warranties, guarantees, or conditions in relation to the application. You may have additional consumer rights under your local laws that this agreement can't change. To the extent permitted under your local laws, Covered Parties exclude any implied warranties or conditions, including those of merchantability, fitness for a particular purpose, safety, comfort, and non-infringement. If your local laws impose a warranty, guarantee or condition even though these terms do not, its duration is limited to 90 days from when you download the application.

11. **LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES.** To the extent not prohibited by law, if you have any basis for recovering damages, you can recover from the application publisher only direct damages up to the amount you paid for the application or \$1.00, whichever is greater. You will not, and waive any right to, seek to recover any other damages, including lost profits and consequential, special, direct, indirect, or incidental damages, from the application publisher.

This limitation applies to:

- Anything related to the application or services made available through the application; and
- Claims for breach of contract, warranty, guarantee or condition; strict liability, negligence, or other tort; violation of a statute or regulation; unjust enrichment; or under any other theory; all to the extent permitted by applicable law.

It also applies even if:

- This remedy doesn't fully compensate you for any losses; or
- The application publisher knew or should have known about the possibility of the damages.

[↑Top of page](#)

Covered Services

The following products, apps and services are covered by the Microsoft Services Agreement, but may not be available in your market.

Account.microsoft.com
Advertising.microsoft.com
Arrow Launcher
Ask Cortana
Bing
Bing Apps

Bing Bots
Bing Desktop
Bing Dictionary
Bing Image Bot
Bing in the Classroom
Bing Input
Bing Maps
Bing Music Bot
Bing Navigation
Bing News Bot
Bing Reader
Bing Rewards
Bing Search app
Bing Toolbar
Bing Torque
Bing Translator
Bing Webmaster
Bing Wikipedia Browser
Bing.com
Bingplaces.com
Choice.microsoft.com
Citizen Next
Conditional Action Programmer
Cortana
Default Homepage and New Tab Page on Microsoft Edge
Dev Center App
Device Health App
Docs.com
Education.minecraft.net
Forzamotorsport.net
Groove
Groove Music Pass
GroupMe
HealthVault
HealthVault Insights
Home
Maps App
Microsoft account
Microsoft Add-Ins for Skype
Microsoft Bots
Microsoft Family
Microsoft Health
Microsoft Movies & TV
Microsoft Support and Recovery Assistant for Office 365
Microsoft Translator
Microsoft Wallpaper
Microsoft XiaoIce
MSN Dial Up
MSN Explorer

MSN Food & Drink
MSN Health & Fitness
MSN Money
MSN News
MSN Premium
MSN Sports
MSN Travel
MSN Weather
MSN.com
News Pro App and Website
Next Lock Screen
Office 365 Consumer
Office 365 Home
Office 365 Personal
Office 365 University
Office Online
Office Store
Office Sway
Office.com
OneDrive
OneDrive.com
OneNote.com
Outlook.com
Paint 3D
Picturesque Lock Screen
Pix Lock
Remix 3D
Seeing AI
Send
Skype
Skype in the Classroom
Skype Manager
Skype Qik
Skype.com
Smart Search
Spreadsheet Keyboard
Store
Sway.com
Todo.microsoft.com
Tossup
Translator
UrWeather
Video Breakdown
Windows Live Mail
Windows Live Writer
Windows Movie Maker
Windows Photo Gallery
Windows Store
Word Flow

Xbox and Windows Games, apps and websites published by Microsoft
Xbox Game Pass
Xbox Live
Xbox Live Gold
Xbox Music
Xbox Store
Zo

[↑Top of page](#)

[English \(United States\)](#)

[Contact us](#)

[Privacy and cookies](#)

[Terms of use](#)

[Trademarks](#)

[About our ads](#)

© 2017 Microsoft



Microsoft Privacy Statement

Last Updated: June 2017 [What's new?](#)

Your privacy is important to us. This privacy statement explains what personal data we collect from you and how we use it. We encourage you to read the summaries below and to click on "Learn More" if you'd like more information on a particular topic.

The product-specific details sections provide additional information relevant to particular Microsoft products. This statement applies to the Microsoft products listed below, as well as other Microsoft products that display this statement. References to Microsoft products in this statement include Microsoft services, websites, apps, software and devices.

Personal Data We Collect

Microsoft collects data to operate effectively and provide you the best experiences with our products. You provide some of this data directly, such as when you create a Microsoft account, submit a search query to Bing, speak a voice command to Cortana, upload a document to OneDrive, purchase an MSDN subscription, sign up for Office 365, or contact us for support. We get some of it by recording how you interact with our products by, for example, using technologies like [cookies](#), and receiving error reports or usage data from software running on your device.

We also obtain data from third parties. We protect data obtained from third parties according to the practices described in this statement, plus any additional restrictions imposed by the source of the data. These third-party sources vary over time, but have included:

- Data brokers from which we purchase demographic data to supplement the data we collect.
- Social networks when you grant permission to a Microsoft product to access your data on one or more networks.
- Service providers that help us determine a location based on your IP address in order to customize certain products to your location.
- Partners with which we offer co-branded services or engage in joint marketing activities, and
- Publicly-available sources such as open government databases or other data in the public domain.

You have choices about the data we collect. When you are asked to provide personal data, you may decline. But if you choose not to provide data that is necessary to provide a product or feature, you may not be able to use that product or feature.

The data we collect depends on the products and features you use, and can include the following:

Name and contact data. We collect your first and last name, email address, postal address, phone number, and other similar contact data.

Credentials. We collect passwords, password hints, and similar security information used for authentication and account access.

Demographic data. We collect data about you such as your age, gender, country, and preferred language.

Payment data. We collect data necessary to process your payment if you make purchases, such as your payment instrument number (such as a credit card number), and the security code associated with your payment instrument.

Device and Usage data. We collect data about your device and how you and your device interact with Microsoft and our products. For example, we collect:

- *Product use data.* We collect data about the features you use, the items you purchase, and the web pages you visit. This data includes your voice and text search queries or commands to Bing, Cortana, and our chat bots.
- *Device, connectivity and configuration data.* We collect data about your device and the network you use to connect to our products. It includes data about the operating systems and other software installed on your device, including product keys. It also includes IP address, device identifiers (such as the IMEI number for phones), regional and language settings.
- *Error reports and performance data.* We collect data about the performance of the products and any problems you experience with them. This data helps us to diagnose problems in the products you use, and to improve our products and provide solutions. Depending on your product and settings, error reports can include data such as the type or severity of the problem, details of the software or hardware related to an error, contents of files you were using when an error occurred, and data about other software on your device.
- *Support Data.* When you engage Microsoft for support, we collect data about you and your hardware, software, and other details related to the support incident. Such data includes contact or authentication data, the content of your chats and other communications with Microsoft support, data about the condition of the machine and the application when the fault occurred and during diagnostics, and system and registry data about software installations and hardware configurations.

Interests and favorites. We collect data about your interests and favorites, such as the teams you follow in a sports app, the stocks you track in a finance app, or the favorite cities you add to a weather app. In addition to those you explicitly provide, your interests and favorites may also be inferred or derived from other data we collect.

Contacts and relationships. We collect data about your contacts and relationships if you use a Microsoft product to manage contacts, or to communicate or interact with other people or organizations.

Location data. We collect data about your location, which can be either precise or imprecise. Precise location data can be Global Position System (GPS) data, as well as data identifying nearby cell towers and Wi-Fi hotspots, we collect when you enable location-based products or features. Imprecise location data includes, for example, a location derived from your IP address or data that indicates where you are located with less precision, such as at a city or postal code level.

Content. We collect content of your files and communications when necessary to provide you with the products you use. For example, if you receive an email using Outlook.com or Exchange Online,

we need to collect the content of that email to deliver it to your inbox, display it to you, enable you to reply to it, and store it for you until you choose to delete it. Examples of this data include: the content of your documents, photos, music, or videos you upload to a Microsoft service such as OneDrive, as well as the content of your communications sent or received using Microsoft products such Outlook.com or Skype, including the:

- subject line and body of an email,
- text or other content of an instant message,
- audio and video recording of a video message, and
- audio recording and transcript of a voice message you receive or a text message you dictate.

We also collect the content of messages you send to us, such as feedback and product reviews you write, or questions and information you provide for customer support. When you contact us, such as for customer support, phone conversations or chat sessions with our representatives may be monitored and recorded. If you enter our retail stores or other facilities, your image may be captured by our security cameras.

Product-specific sections below describe data collection practices applicable to use of those products.

How We Use Personal Data

Microsoft uses the data we collect for three basic purposes, described in more detail below: (1) to operate our business and provide (including improving and personalizing) the products we offer, (2) to send communications, including promotional communications, and (3) for some products, to show advertising.

In carrying out these purposes, we combine data we collect to give you a more seamless, consistent and personalized experience. For example, [Cortana](#) can use the favorite sports teams you add to the Microsoft Sports app to provide information relevant to your interests, or [Windows Store](#) can use information about the apps and services you use to make personalized app recommendations. However, to enhance privacy, we have built in technological and procedural safeguards designed to prevent certain data combinations. For example, we store data we collect from you when you are unauthenticated (not signed in) separately from any account information that directly identifies you, such as your name, email address or phone number.

Providing and improving our products. We use data to provide and improve the products we offer and perform essential business operations. This includes operating the products, maintaining and improving the performance of the products, including developing new features, research, and providing customer support. Examples of such uses include the following.

- **Providing the Products.** We use data to carry out your transactions with us and to provide our products to you. Often, those products include personalized features and recommendations that enhance your productivity and enjoyment, and automatically tailor your product experiences based on the data we have about your activities, interests and location.
- **Customer support.** We use data to diagnose product problems, repair customers' devices, and provide other customer care and support services.
- **Product activation.** We use data - including device and application type, location, and unique device, application, network and subscription identifiers - to activate software and devices that require activation.

- **Product Improvement.** We use data to continually improve our products, including adding new features or capabilities, such as using error reports to improve security features, using search queries and clicks in Bing to improve the relevancy of the search results, using usage data to determine what new features to prioritize, or using audio recordings from voice input features to improve speech recognition accuracy.
- **Security, Safety and Dispute Resolution.** We use data to protect the security and safety of our products and our customers, to detect and prevent fraud, to confirm the validity of software licenses, to resolve disputes and enforce our agreements. Our security features and products can disrupt the operation of malicious software and notify users if malicious software is found on their devices. For example, many of our communications and file syncing products systematically scan content in an automated manner to identify suspected spam, viruses, abusive actions, or URLs that have been flagged as fraud, phishing or malware links; and we may block delivery of a communication or remove content if it violates our terms.
- **Business Operations.** We use data to develop aggregate analysis and business intelligence that enable us to operate, protect, make informed decisions, and report on the performance of our business.

Communications. We use data we collect to deliver and personalize our communications with you. For example, we may contact you by email or other means to inform you when a subscription is ending, let you know when security updates are available, remind you about items left in your online shopping cart, update you or inquire about a service or repair request, invite you to participate in a survey, or tell you that you need to take action to keep your account active. Additionally, you can sign up for email subscriptions and choose whether you wish to receive promotional communications from Microsoft by email, SMS, physical mail, and telephone. For information about managing email subscriptions and promotional communications, please visit the [Access and Controls](#) section of this privacy statement.

Advertising. Many of our products are supported by advertising. We share the data we collect with third parties such as AOL and AppNexus so that they can select and deliver some of the ads you see on our sites and apps, as well as other sites and apps serviced by these partners. The ads that you see may be selected based on your current location, search query, or the content you are viewing. Other ads are targeted based on your likely interests or other information learned about you over time using demographic data, search queries, interests and favorites, usage data from our own sites and apps and the sites and apps of our advertisers and partners, and location data - which we refer to as "interest-based advertising" in this statement. To provide interest-based advertising, we combine cookies placed on your device using information that we collect (such as IP address) when your browser interacts with our websites. If you opt out of receiving interest-based advertising, data associated with these cookies will not be used. Microsoft does not use what you say in email, chat, video calls or voice mail, or your documents, photos or other personal files to target ads to you. **You can opt out of receiving interest-based advertising from Microsoft by visiting our [opt-out page](#).** More information about advertising controls is available in the [Access and Controls](#) section of this privacy statement. Further details regarding our advertising-related uses of data include:

- **Advertising Industry Best Practices and Commitments.** Microsoft is a member of the [Network Advertising Initiative](#) (NAI) and adheres to the NAI Code of Conduct. We also adhere to the following self-regulatory programs:
 - In the US: [Digital Advertising Alliance \(DAA\)](#)
 - In Europe: [European Interactive Digital Advertising Alliance \(EDAA\)](#)

- In Canada: [Ad Choices: Digital Advertising Alliance of Canada \(DAAC\)](#) / [Choix de Pub: l'Alliance de la publicité numérique du Canada \(DAAC\)](#)
- **Health-Related Ad Targeting.** In the United States, we provide interest-based advertising based on a limited number of standard, non-sensitive health-related interest categories, including allergies, arthritis, cholesterol, cold and flu, diabetes, gastrointestinal health, headache / migraine, healthy eating, healthy heart, men's health, oral health, osteoporosis, skin health, sleep, and vision / eye care. We will also target ads based on custom, non-sensitive health-related interest categories as requested by advertisers.
- **Children and Advertising.** We do not deliver interest-based advertising to children whose birthdate in their Microsoft account identifies them as under 13 years of age.
- **Data Retention.** For interest-based advertising, we retain data for no more than 13 months, unless we obtain your consent to retain the data longer.
- **Data Sharing.** In some cases, we share with advertisers reports about the data we have collected on their sites or ads. Advertisers may choose to place our [web beacons](#) on their sites in order to allow Microsoft to collect information on their sites such as activities, purchases and visits; we use this data on behalf of our advertising customers to help target their ads. We also share data directly with service providers (such as AOL and AppNexus) to permit them to provide services on our behalf or to partner with us in selecting and serving ads for our advertising partners.
- **Data Collected by Other Advertising Companies.** Advertisers sometimes include their own [web beacons](#) (or those of their other advertising partners) within their advertisements that we display, enabling them to set and read their own [cookie](#). Additionally, Microsoft partners with third-party ad companies to help provide some of our advertising services, and we also allow other third-party ad companies to display advertisements on our sites. These third parties may place cookies on your computer and collect data about your online activities across websites or online services. These companies currently include, but are not limited to: [A9](#), [AOL Advertising](#), [AppNexus](#), [Criteo](#), [Facebook](#), [MediaMath](#), [nugg.adAG](#), [Rocket Fuel](#), [Yahoo!](#). You may find more information on each company's practices, including the choices it offers, by clicking on the company names above. Many of them are also members of the [NAI](#) or [DAA](#), which each provide a simple way to opt out of ad targeting from participating companies.

Reasons We Share Personal Data

We share your personal data with your consent or as necessary to complete any transaction or provide any product you have requested or authorized. For example, we share your content with third parties when you tell us to do so, such as when you send an email to a friend, share photos and documents on OneDrive, or link accounts with another service. When you provide payment data to make a purchase, we will share payment data with banks and other entities that process payment transactions or provide other financial services, and for fraud prevention and credit risk reduction.

In addition, we share personal data among Microsoft-controlled affiliates and subsidiaries. We also share personal data with vendors or agents working on our behalf for the purposes described in this statement. For example, companies we've hired to provide customer service support or assist in protecting and securing our systems and services may need access to personal data in order to provide those functions. In such cases, these companies must abide by our data privacy and security requirements and are not allowed to use personal data they receive from us for any other purpose. We may also disclose personal data as part of a corporate transaction such as a merger or sale of assets.

Finally, we will access, transfer, disclose, and preserve personal data, including your content (such as the content of your emails in Outlook.com, or files in private folders on OneDrive), when we have a good faith belief that doing so is necessary to:

1. comply with applicable law or respond to valid legal process, including from law enforcement or other government agencies;
2. protect our customers, for example to prevent spam or attempts to defraud users of our products, or to help prevent the loss of life or serious injury of anyone;
3. operate and maintain the security of our products, including to prevent or stop an attack on our computer systems or networks; or
4. protect the rights or property of Microsoft, including enforcing the terms governing the use of the services - however, if we receive information indicating that someone is using our services to traffic in stolen intellectual or physical property of Microsoft, we will not inspect a customer's private content ourselves, but we may refer the matter to law enforcement.

For more information about data we disclose in response to requests from law enforcement and other government agencies, please see our Law Enforcement Transparency Report, available at microsoft.com/about/corporatecitizenship/en-us/reporting/transparency.

Please note that some of our products include links to products of third parties whose privacy practices differ from Microsoft's. If you provide personal data to any of those products, your data is governed by their privacy statements.

How to Access & Control Your Personal Data

You can view, edit, or delete your personal data online for many Microsoft products. You can also make choices about Microsoft's collection and use of your data. How you can access or control your personal data will depend on which products you use. For example:

- **Microsoft privacy dashboard.** You can see and control activity data across multiple Microsoft services on the Microsoft privacy dashboard at: account.microsoft.com/privacy. From here, you can view, and clear browsing, search, and location data associated with your Microsoft account. You can also manage data in your Cortana Notebook and Microsoft Health services.
- **Microsoft account.** If you wish to access, edit, or remove the profile information and payment information in your [Microsoft account](#), change your password, add security information or close your account, you can do so by visiting account.microsoft.com. From here, you can also access controls for other Microsoft products.
- **Skype.** If you wish to access edit or remove profile information and payment information in your Skype account or change your password, you can sign into your account at login.skype.com/login.
- **Xbox.** If you use Xbox Live or Xbox.com, you can view or edit your personal data, including billing and account information, privacy settings, online safety and data sharing preferences by accessing [My Xbox](#) on the Xbox console or on the Xbox.com website.
- **Microsoft Store.** You can access your Microsoft Store profile and account information by visiting www.microsoftstore.com/ and clicking on "View account" or "Order history."
- **Microsoft.com.** You can access and update your profile on microsoft.com by visiting the [Microsoft.com Profile Center](#). If you have a Microsoft Developer Network public profile, you can access and edit it at connect.microsoft.com/profile.aspx.

If you cannot access certain personal data collected by Microsoft via the links above or directly through the Microsoft products you use, you can always contact Microsoft by using our [web form](#). We will respond to requests to access or delete your personal data within 30 days.

Your Communications Preferences

You can choose whether you wish to receive promotional communications from Microsoft by email, SMS, physical mail, and telephone. If you receive promotional email or SMS messages from us and would like to opt out, you can do so by following the directions in that message. You can also make choices about the receipt of promotional email, telephone calls, and postal mail by signing in with your personal [Microsoft account](#), and viewing your [communication permissions](#) where you can update contact information, manage Microsoft-wide contact preferences, opt out of email subscriptions, and choose whether to share your contact information with Microsoft partners. If you do not have a personal Microsoft account, you can manage your Microsoft email contact preferences by using this [web form](#). These choices do not apply to mandatory service communications that are part of certain Microsoft services, or to surveys or other informational communications that have their own unsubscribe method.

Your Advertising Choices

You may opt out of receiving interest-based advertising from Microsoft by visiting our [opt-out page](#). When you opt out, your selection will be stored in a [cookie](#) that is specific to the web browser you are using. The opt-out cookie has an expiration date of five years. If you delete the cookies on your device, you will need to opt out again.

You can also link your opt-out choice with your personal Microsoft account. It will then apply on any device where you use that account, and will continue to apply until someone signs in with a different personal Microsoft account on that device. If you delete the cookies on your device, you will need to sign in again for the settings to apply.

For advertising that appears in apps on Windows, you may use the opt-out linked to your personal Microsoft account, or opt out of interest-based advertising by turning off the [advertising ID](#) in Windows Settings.

Because the data used for interest-based advertising is also used for other necessary purposes (including providing our products, analytics and fraud detection), opting out of interest-based advertising does not stop that data from being collected. Nor does it mean you will stop getting ads or see fewer ads. However, if you do opt out, the ads you receive will no longer be interest-based and may be less relevant to your interests.

Browser-Based Controls

- **Cookie Controls.** Relevant browser-based cookie controls are described in the [Cookies](#) section of this privacy statement.
- **Tracking Protection.** Internet Explorer (versions 9 and up) has a feature called Tracking Protection that will block third-party content, including cookies, from any site that is listed in a Tracking Protection List you add. By limiting calls to these sites, the browser will limit the information these third-party sites can collect about you.
- **Browser Controls for "Do Not Track."** Some browsers have incorporated "Do Not Track" (DNT) features that can send a signal to the websites you visit indicating you do not

wish to be tracked. Because there is not yet a common understanding of how to interpret the DNT signal, Microsoft services do not currently respond to browser DNT signals. We continue to work with the online industry to define a common understanding of how to treat DNT signals. In the meantime, you can use the range of other tools we provide to control data collection and use, including the ability to opt out of receiving interest-based advertising from Microsoft as described above.

Cookies & Similar Technologies

Microsoft uses cookies (small text files placed on your device) and similar technologies to provide our websites and online services and to help collect data. The text in a cookie often consists of a string of numbers and letters that uniquely identifies your computer, but it can contain other information as well. Microsoft apps use other identifiers, such as the [advertising ID](#) in Windows, for similar purposes, and many of our websites and applications also contain web beacons or other similar technologies, as described below.

Our Use of Cookies and Similar Technologies

Microsoft uses cookies and similar technologies for several purposes, depending on the product, including:

- **Storing your Preferences and Settings.** Settings that enable our products to operate correctly or that maintain your preferences over time may be stored on your device. For example, if you enter your city or postal code to get local news or weather information on a Microsoft website, we may store that data in a cookie so that you will see the relevant local information when you return to the site. If you opt out of interest-based advertising, we store your opt-out preference in a cookie on your device.
- **Sign-in and Authentication.** When you sign into a website using your personal [Microsoft account](#), we store a unique ID number, and the time you signed in, in an encrypted cookie on your device. This cookie allows you to move from page to page within the site without having to sign in again on each page.
- **Interest-Based Advertising.** Microsoft uses cookies to collect data about your online activity and identify your interests so that we can provide advertising that is most relevant to you. You can opt out of receiving interest-based advertising from Microsoft as described in the [Access and Control](#) section of this privacy statement.
- **Analytics.** In order to provide our products, we use cookies and other identifiers to gather usage and performance data. For example, we use cookies to count the number of unique visitors to a web page or service and to develop other statistics about the operations of our products.

Some of the cookies we commonly use are listed in the following chart. This list is not exhaustive, but it is intended to illustrate the main reasons we typically set cookies. If you visit one of our websites, the site may set some or all of the following cookies:

Cookie name	Description
MUID	Identifies unique web browsers visiting Microsoft sites. It is used for advertising, site analytics and other operational purposes.

ANON	Contains the ANID, a unique identifier derived from your Microsoft account, which is used for advertising, personalization, and operational purposes. It is also used to preserve your choice to opt out of interest-based advertising from Microsoft, if you have chosen to associate the opt-out with your Microsoft account.
CC	Contains a country code as determined from your IP address.
RPSTAuth, MSNRPSAuth, KievRPSAuth	Helps to authenticate you when you sign in with your Microsoft account.
NAP	Contains an encrypted version of your country, postal code, age, gender, language and occupation, if known, based on your Microsoft account profile.
MH	Appears on co-branded sites where Microsoft is partnering with an advertiser. This cookie identifies the advertiser so the right ad is selected.
TOptOut	Records your decision not to receive interest-based advertising delivered by Microsoft.

In addition to the cookies Microsoft sets when you visit our websites, third parties may also set cookies when you visit Microsoft sites. In some cases, that is because we have hired the third party to provide services on our behalf, such as site analytics. In other cases, it is because our web pages contain content or ads from third parties, such as videos, news content or ads delivered by other ad networks. Because your browser connects to those third parties' web servers to retrieve that content, those third parties are able to set or read their own cookies on your device and may collect information about your online activities across websites or online services.

How to Control Cookies

Most web browsers automatically accept cookies but provide controls that allow you to block or delete them. For example, in Microsoft Edge, you can block or delete cookies by clicking **Settings > Privacy > Cookies**. Instructions for blocking or deleting cookies in other browsers may be available in each browser's privacy or help documentation.

Certain features of Microsoft products depend on cookies. Please be aware that if you choose to block cookies, you may not be able to sign in or use those features, and preferences that are dependent on

cookies may be lost. If you choose to delete cookies, settings and preferences controlled by those cookies, including advertising preferences, will be deleted and may need to be recreated.

Additional privacy controls that can impact cookies, including the Tracking Protection feature of Microsoft browsers, are described in the [Access and Control](#) section of this privacy statement.

Our Use of Web Beacons and Analytics Services

Microsoft web pages may contain electronic images known as web beacons (also called single-pixel gifs) that we use to help deliver cookies on our websites, count users who have visited those websites and deliver co-branded products. We also include web beacons in our promotional email messages or newsletters to determine whether you open and act on them.

In addition to placing web beacons on our own websites, we sometimes work with other companies to place our web beacons on their websites or in their advertisements. This helps us develop statistics on how often clicking on an advertisement on a Microsoft website results in a purchase or other action on the advertiser's website.

Finally, Microsoft products often contain web beacons or similar technologies from third-party analytics providers, which help us compile aggregated statistics about the effectiveness of our promotional campaigns or other operations. These technologies enable the analytics providers to set or read their own cookies or other identifiers on your device, through which they can collect information about your online activities across applications, websites or other products. However, we prohibit these analytics providers from using web beacons on our sites to collect or access information that directly identifies you (such as your name or email address). You can opt out of data collection or use by some of these analytics providers by clicking the following links:

- AppsFlyer: www.appsflyer.com/optout
- Flurry Analytics: dev.flurry.com/secure/optOut.do
- Google Analytics: tools.google.com/dlpage/gaoptout (requires you to install a browser add-on)
- Kissmetrics: kissmetrics.com/user-privacy
- Mixpanel: mixpanel.com/optout
- Nielsen: www.nielsen-online.com/corp.jsp?section=leg_prs&nav=1#Optoutchoices
- Omniture (Adobe): www.d1.sc.omtrdc.net/optout.html
- Visible Measures: www.visiblemeasures.com/viewer-settings-opt-out
- WebTrends: ondemand.webtrends.com/support/optout.asp

Other Similar Technologies

In addition to standard cookies and web beacons, our products can also use other similar technologies to store and read data files on your computer. This is typically done to maintain your preferences or to improve speed and performance by storing certain files locally. But, like standard cookies, these technologies can also be used to store a unique identifier for your computer, which can then be used to track behavior. These technologies include Local Shared Objects (or "Flash cookies") and Silverlight Application Storage.

Local Shared Objects or "Flash cookies." Web sites that use Adobe Flash technologies can use Local Shared Objects or "Flash cookies" to store data on your computer. To manage or block Flash cookies, go to www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html.

Silverlight Application Storage. Web sites or applications that use Microsoft Silverlight technology also have the ability to store data by using Silverlight Application Storage. To learn how to manage or block such storage, see the [Silverlight](#) section of this statement.

Microsoft account

With a Microsoft account, you can sign into Microsoft products, as well as those of select Microsoft partners. When you create your own Microsoft account, we refer to that account as a personal Microsoft account. When you sign into products that use Microsoft Azure Active Directory (AAD) with an email address from your employer or school, we refer to that account as a work or school account.

Creating and using your personal Microsoft account. When you create a personal Microsoft account, you will be asked for certain personal data and we will assign a unique ID number to identify your account and associated information. While some products, such as those involving payment, require a real name, you can sign into and use some Microsoft products without providing your real name. Some data you provide, such as your display name, email address and phone number, can be used to help others find and connect with you within Microsoft products. For example, people who know your display name, email address or phone number can use it to search for you on Skype and send you an invite to connect with them. Note that if you use a work or school email address to create a personal Microsoft account, and your employer or school that issued that address begins managing that account with Azure Active Directory (AAD), you will need to update the email address associated with your personal Microsoft account in order to continue accessing Microsoft products that do not use AAD (such as Xbox Live).

Signing in. When you sign into your Microsoft account, we create a record of your sign-in, which includes the date and time, information about the product you signed into, your sign-in name, the unique number assigned to your account, a unique identifier assigned to your device, your IP address, and your operating system and browser version.

Signing into Microsoft. Signing into your account enables improved personalization, provides seamless and consistent experiences across products and devices, permits you to access and use cloud data storage, allows you to make payments using payment instruments stored in your Microsoft account, and enables other enhanced features and settings. When you sign into your account, you will stay signed in until you sign out. If you add your Microsoft account to a Windows device (version 8 or higher), Windows will automatically sign you into products that use Microsoft account that you access on that device. When you are signed in, some products will display your name or username and your profile photo (if you have added one to your profile) as part of your use of Microsoft products, including in your communications, social interactions and public posts.

Signing into third-party products. If you sign into a third-party product with your Microsoft account, you will be asked to consent to share the account data required by that product. The third party will also receive the version number assigned to your account (a new version number is assigned each time you change your sign-in data); and whether your account has been deactivated. If you have consented to share your profile data, the third party may display your name or username and your profile photo (if you have added one to your profile) when you are signed in to that third-party product. If you chose to make payments to third-party merchants using your Microsoft account, Microsoft will pass to the third party information stored in your Microsoft account necessary to process your payment and fulfill your order (such as name, credit card number, billing and shipping

addresses, and relevant contact information). The third party can use or share the data it receives when you sign in or make a purchase according to its own practices and policies. **You should carefully review the privacy statement for each product you sign into and each merchant you purchase from to determine how it will use the data it collects.**

Personal Microsoft accounts received from third parties. If you received your personal Microsoft account from a third party, like an Internet service provider, that third party may have rights over your account, including the ability to access or delete your Microsoft account. **You should carefully review any additional terms the third party provided you to understand what it can do with your account.**

Connecting your personal Microsoft account to your social network accounts. You may connect your personal Microsoft account to your accounts on social networks such as Facebook, Twitter, or LinkedIn in order to access data from those social networks from within Microsoft products. If you choose to do so, we will store data about your social network accounts on our servers so that we can display updated data from your social network account. You can disconnect a social network account from your personal Microsoft account at any time at profile.live.com/services.

Using work or school accounts. If your employer or school uses Azure Active Directory (AAD) to issue and manage the account it provides you, you can use your work or school account to sign into Microsoft products that use AAD (such as Office 365 or Skype for Business). If required by your organization, you will also be asked to provide a phone number or an alternative email address for additional security verification. If you sign into Microsoft products with a work or school account, the owner of the domain associated with your email address may control and administer your account, and access and process your data, including the contents of your communications and files. Your use of the products may be subject to your organization's policies, if any. Microsoft is not responsible for the privacy or security practices of these organizations, which may differ from those of Microsoft. If your organization is administering your use of Microsoft products, please direct your privacy inquiries to your administrator.

Other Important Privacy Information

Below you will find additional privacy information you may find important. You can also find more information on Microsoft's commitment to protecting your privacy at privacy.microsoft.com.

European Privacy Rights

Microsoft adheres to applicable data protection laws in the European Economic Area, which if applicable includes the following rights:

- If the processing of personal data is based on your consent, you have a right to withdraw consent at any time for future processing;
- You have a right to request from us, a “data controller” as defined in the law, access to and rectification of your personal data;
- You have a right to object to the processing of your personal data; and
- You have a right to lodge a complaint with a data protection authority.

As applicable under French law, you can also send us specific instructions regarding the use of your personal data after your death, by using our [web form](#).

When we process personal data about you, we do so with your consent and/or as necessary to provide the products you use, operate our business, meet our contractual and legal obligations, protect the security of our systems and our customers, or fulfill other legitimate interests of Microsoft as described in the “How We Use Personal Data” and “Reasons We Share Personal Data” sections above. When we transfer personal data from the European Economic Area, we do so based on a variety of legal mechanisms, as described in “Where We Store and Process Personal Data” below.

Security of Personal Data

Microsoft is committed to protecting the security of your personal data. We use a variety of security technologies and procedures to help protect your personal data from unauthorized access, use or disclosure. For example, we store the personal data you provide on computer systems that have limited access and are in controlled facilities. When we transmit highly confidential data (such as a credit card number or password) over the Internet, we protect it through the use of encryption.

Where We Store and Process Personal Data

Personal data collected by Microsoft may be stored and processed in your region, in the United States or in any other country where Microsoft or its affiliates, subsidiaries or service providers maintain facilities. Microsoft maintains major data centers in the United States, Canada, Brazil, Ireland, the Netherlands, Austria, Finland, India, Singapore, Malaysia, Hong Kong, Japan, and Australia. Typically, the primary storage location is in the customer’s region or in the United States, often with a backup to a data center in another region. The storage location(s) are chosen in order to operate efficiently, to improve performance, and to create redundancies in order to protect the data in the event of an outage or other problem. We take steps to ensure that the data we collect under this privacy statement is processed according to the provisions of this statement and the requirements of applicable law wherever the data is located.

When we transfer personal data from the European Economic Area and Switzerland to other countries, some of which have not been determined by the European Commission to have an adequate level of data protection. When we do, we use a variety of legal mechanisms, including contracts, to help ensure your rights and protections travel with your data.

Microsoft Corporation and its controlled U.S. subsidiaries also participate in the EU-U.S. Privacy Shield framework and will participate in the Swiss-U.S. Privacy Shield framework when it becomes available as of April 2017. Microsoft adheres to the principles of each Privacy Shield with respect to personal data transferred from the European Economic Area and Switzerland. If third-party agents process personal data on our behalf in a manner inconsistent with the principles of either Privacy Shield framework, we remain liable unless we prove we are not responsible for the event giving rise to the damage. The U.S. Department of Commerce lists the participants of each Privacy Shield at [privacyshield.gov](https://www.privacyshield.gov).

If you have a question or complaint related to Microsoft’s participation in the EU-U.S. or Swiss-U.S. Privacy Shield, we encourage you to contact us via our [web form](#). For any complaints related to the Privacy Shield frameworks that cannot be resolved with Microsoft directly, we have chosen to cooperate with the relevant Data Protection Authority, or a panel

established by the European DPAs for resolving disputes. Please contact us to be directed to the relevant DPA contacts. As further explained in the Privacy Shield Principles, binding arbitration is available to address residual complaints not resolved by other means. Microsoft is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission (FTC).

Our Retention of Personal Data

Microsoft retains personal data for as long as necessary to provide the products and fulfill the transactions you have requested, or for other essential purposes such as complying with our legal obligations, resolving disputes, and enforcing our agreements. Because these needs can vary for different data types in the context of different products, actual retention periods can vary significantly. The criteria used to determine the retention periods include:

- *How long is the personal data needed to provide the products and operate our business?* This includes such things as maintaining and improving the performance of those products, keeping our systems secure, and maintaining appropriate business and financial records. This is the general rule that establishes the baseline for most data retention periods.
- *Do customers provide, create, or maintain the data with the expectation we will retain it until they affirmatively remove it?* Examples include a document you store in OneDrive, or an email message you keep in your Outlook.com inbox. In such cases, we maintain the data until you actively delete it, such as by moving an email from your Outlook.com inbox to the Deleted Items folder, and then emptying that folder (when your Deleted Items folder is emptied, those emptied items remain in our system for up to 30 days before final deletion).
- *Is there an automated control, such as in the Microsoft privacy dashboard, that enables the customer to access and delete the personal data at any time?* If there is not, a shortened data retention time will generally be adopted.
- *Is the personal data of a sensitive type?* If so, a shortened retention time would generally be appropriate.
- *Has Microsoft adopted and announced a specific retention period for a certain data type?* For example, for Bing search queries, we de-identify stored queries by removing the entirety of the IP address after 6 months, and cookie IDs and other cross-session identifiers after 18 months.
- *Has the user provided consent for a longer retention period?* If so, we will retain data in accordance with your consent.
- *Is Microsoft subject to a legal, contractual, or similar obligation to retain the data?* Examples can include mandatory data retention laws in the applicable jurisdiction, government orders to preserve data relevant to an investigation, or data that must be retained for the purposes of litigation.

Collection of Data From Children

When a Microsoft product collects age it will either block users under 13 or will ask them to provide consent from a parent or guardian before they can use it. We will not knowingly ask children under 13 to provide more data than is necessary to provide the product.

Once parental consent is granted, the child's account is treated much like any other account. The child may have access to communication services like email, instant messaging and online message boards and may be able to communicate freely with other users of all ages.

Parents can change or revoke the consent choices previously made, and review, edit or request the deletion of their children's personal data. For example, parents can access their personal [Microsoft account](#) and click on "Permissions." For users of Minecraft and other Mojang games, parents can contact us at account.mojang.com/terms#contact.

Preview Releases

Microsoft offers preview, insider, beta or other pre-release products and features ("previews") to enable you to evaluate them while providing feedback, including performance and usage data, to Microsoft. As a result, previews can automatically collect additional data, provide fewer controls, and otherwise employ different privacy and security measures than those typically present in our products. If you participate in previews, we may contact you about your feedback or your interest in continuing to use the product after general release.

Changes to This Privacy Statement

We will update this privacy statement when necessary to reflect customer feedback and changes in our products. When we post changes to this statement, we will revise the "last updated" date at the top of the statement and describe the changes in the [Change History](#) page. If there are material changes to the statement or in how Microsoft will use your personal data, we will notify you either by prominently posting a notice of such changes before they take effect or by directly sending you a notification. We encourage you to periodically review this privacy statement to learn how Microsoft is protecting your information.

How to Contact Us

If you have a technical or support question, please visit support.microsoft.com to learn more about Microsoft Support offerings. If you have a personal Microsoft account password question, please visit [Microsoft account support](#).

If you have a privacy concern or a question for the Chief Privacy Officer/Data Protection Officer of Microsoft, please contact us by using our [Web form](#). We will respond to questions or concerns within 30 days.

Unless otherwise stated, Microsoft Corporation is a data controller for personal data we collect through the products subject to this statement. Our address is Microsoft Privacy, Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052, USA. Telephone: (+1) 425-882-8080.

Microsoft Ireland Operations Limited is our data protection representative for the European Economic Area and Switzerland. The data protection officer of Microsoft Ireland Operations Limited can be reached at the following address: Microsoft Ireland Operations, Ltd., Attn: Data Protection, Carmenhall Road, Sandyford, Dublin 18, Ireland.

Skype Communications S.à.r.l. 23-29 Rives de Clausen L-2165 Luxembourg, Luxembourg is a data controller for Skype. To contact us in relation to Skype software or products, please submit a support request to the Skype [customer support team](#).

To find the Microsoft subsidiary in your country or region, see www.microsoft.com/worldwide/.

Bing

Bing services include search and mapping services, as well as the Bing Toolbar and Bing Desktop apps. Bing services are also included within other Microsoft services, such as [MSN Apps](#) and [Cortana](#), and certain features in [Windows](#) (which we refer to as Bing-powered experiences).

When you conduct a search, or use a feature of a Bing-powered experience that involves conducting a search or entering a command on your behalf, Microsoft will collect the search or command terms you provide, along with your IP address, location, the unique identifiers contained in our [cookies](#), the time and date of your search, and your browser configuration. If you use Bing voice-enabled services, additionally your voice input and performance data associated with the speech functionality will be sent to Microsoft. When you use Bing-powered experiences, such as Ask Cortana or Bing Lookup, to search a particular word or phrase within a web page or document, that word or phrase is sent to Bing along with some surrounding content in order to provide contextually relevant search results.

Search Suggestions. For the Search Suggestions feature, the characters that you type into a Bing-powered experience to conduct a search will be sent to Microsoft. This allows us to provide you with suggestions as you type your searches. To turn this feature on or off, while using Bing Search, go to [Bing settings](#). Search Suggestions cannot be turned off in Cortana. On Windows, you can always hide Cortana and the search box so as not to use the feature.

Bing Experience Improvement Program for Bing Desktop and Bing Toolbar. If you are using Bing Desktop or Bing Toolbar and choose to participate in the Bing Experience Improvement Program, we also collect additional data about how you use these specific Bing apps, such as the addresses of the websites you visit, to help improve search ranking and relevance. To help protect your privacy, we do not use the data collected through the Bing Experience Improvement Program to identify or contact you, or target advertising to you. You can turn off the Bing Experience Improvement Program at any time in the Bing Desktop or Bing Toolbar settings. Finally, we delete the information collected through the Bing Experience Improvement Program after 18 months.

Retention and de-identification. We de-identify stored search queries by removing the entirety of the IP address after 6 months, and cookie IDs and other cross-session identifiers after 18 months.

Personalization through Microsoft account. Some Bing services provide you with an enhanced experience when you sign in with your personal [Microsoft account](#), for example, syncing your search history across devices. You can use these personalization features to customize your interests, favorites, and settings, and to connect your account with third-party services. Visit the [Bing Settings](#) page to manage your personalization settings or the Microsoft privacy dashboard.

Managing Search History. Bing's Search History service provides an easy way to revisit the search terms you've entered and results you've clicked when using Bing search through your browser. You may clear your search history on the Microsoft privacy dashboard at account.microsoft.com/privacy. Clearing your history removes it from the Search History service and prevents that history from being

displayed on the site, but does not delete information from our search logs, which are retained and de-identified as described above.

Non-Microsoft services that use Bing. You may access Bing-powered experiences when using other non-Microsoft services, such as those from Yahoo!. In order to provide these services, Bing receives data from these and other partners that may include date, time, IP address, a unique identifier and other search-related data. This data will be sent to Microsoft in order to provide the search service. Microsoft will use this data as described in this statement or as further limited by our contractual obligations with our partners. You should refer to the privacy policies of the non-Microsoft services for any questions about how they collect and use data.

Search query passed in referral URL. When you click on a search result or advertisement from a Bing search results page and go to the destination website, the destination website will receive the standard data your browser sends to every web site you visit - such as your IP address, browser type and language, and the URL of the site you came from (in this case, the Bing search results page). Because the URL of the Bing search results page contains the text of the search query you entered (which could include names, addresses, or other identifying information), the destination website will be able to determine the search term you entered.

If your browser is enabled to allow pages to pre-load in the background for faster performance, when your browser loads a page in the background, it will have the same effect as if you visited that page, including sending the Bing search results page URL (containing your search query) and downloading any [cookies](#) that page sets.

Sharing search data for research and development purposes. We share some de-identified search query data, including voice queries, with selected third parties for research and development purposes. Before we do so, we remove all unique identifiers such as IP addresses and cookie IDs from the data. We also run the data through a process designed to remove certain sensitive data that users may have included in the search terms themselves (such as social security numbers or credit card numbers). Additionally, we require these third parties to keep the data secure and to not use the data for other purposes.

Cortana

Cortana is your personal assistant. Depending on the capabilities of your device and the version of Cortana you are using. (e.g., Windows, Xbox, iOS, etc.) Cortana can provide a range of features, some of them personalized. Cortana works best when you sign in and let her use data from your device, your personal Microsoft account or your work or school account, other Microsoft services, and third-party services you choose to connect. On Windows devices, if you choose not to sign into Cortana, you can still chat with Cortana and use Cortana to help you search the web, or for your documents stored in Microsoft services like OneDrive and on your device. See the subsection on [Windows Search](#) for more information. But if you don't sign in, your experiences will be more limited and will not be personalized. On iOS and Android devices, Cortana works only when you sign-in.

Signed out. When you are not signed in on a Windows device, Cortana will collect data about how you chat with Cortana and use Cortana to search, using either your voice, inking, or typing. This data includes the following:

- **Speech Services.** To help Cortana better understand the way you speak and your voice commands, speech data is sent to Microsoft to build speech models and improve speech recognition and user intent understanding. If you choose to sign in, the speech models will become more personalized.
- **Queries and search history.** Your Bing search queries and the Search Suggestion feature - even if Cortana does the searching for you - are treated like any other Bing search queries and are used as described in the [Bing](#) section.
- **Device Data.** Cortana can access data about your device and how you use it. For instance, it can determine if Bluetooth is on, whether your lock screen is on, your alarm settings, and which apps you install and use.

Signed in. If you sign in, you enable Cortana to perform additional tasks and to provide personalized experiences and relevant suggestions; and you give Cortana permission to collect or access the following additional types of data, some of which depend on the capabilities of the version of Cortana you are using (e.g., Windows, Android, iOS, etc.) and the app you are using into which Cortana is integrated (e.g. Skype):

- **Microsoft account.** Cortana can access the demographic data (such as your age, postal code and gender) you provided when you created your personal [Microsoft account](#).
- **Other Microsoft product usage.** Cortana uses data collected through other Microsoft services to provide personalized suggestions. For example, Cortana uses data collected by the Sports app, so it can automatically display information about the teams you follow. It also learns your favorite places from Microsoft's Maps app, your favorite songs and artists from the music you play in [Groove Music](#), and what you view and purchase in the [Windows Store](#) so it can offer better suggestions. Your interests in Cortana's Notebook can be used by other Microsoft services, such as Bing or MSN, to customize your interests, preferences, and favorites in those experiences as well.

Location. You can choose whether Cortana accesses your location information in order to give you the most relevant notices and results and to make suggestions that help save you time, such as traffic information and location-based reminders. If you grant permission, Cortana will regularly collect and use your current location, location history, and other location signals (such as locations tagged on photos you upload to OneDrive). Location information collected by Cortana may also be used in de-identified form to improve the Windows Location Services. See more details in the [Location Services](#) subsection.

Contacts, email, calendar & communications. You can choose to let Cortana access your device and cloud-based email and other communications, your calendar, and your contacts in order to enable additional features and personalization. If you give permission, Cortana will access additional data including:

- **Text messages and email.** Cortana accesses your messages to do a variety of things such as: allowing you to add events to your calendar, apprising you of important messages, and keeping you up to date on events or other things that are important to you, like package or flight tracking. Cortana also uses your messages to help you with planning around your events and offers other helpful suggestions and recommendations.
- **Communications History.** Cortana learns who is most important to you from your call, text message, and email history. This data is used to keep track of people most relevant to you and your preferred methods of communication, flag important messages for you (such as missed calls), and improve the performance of Cortana features such as speech recognition.

- **Calendar appointments.** Cortana access your calendars in order to provide reminders and information relevant to your appointments.

Browsing history. If you allow Cortana to use your browsing history, Microsoft will collect your Microsoft Edge search queries and full browsing history, associated with a user ID. Cortana will use this data to learn about you and provide you with timely and intelligent answers and proactive personalized suggestions, or to complete web tasks for you. Cortana won't collect information about sites you visit in InPrivate tabs.

Other Connected Services and managing Skills. You can also give Cortana access to data collected by other Microsoft and third-party services, or share your Cortana information with those services, by giving your permission to enable or connect those services with Cortana. When you enable a Connected Service or third-party Skill, Cortana shares your request with those services or third parties to enable your command; Cortana may also share additional information that you give permission to share (e.g., your location). Below are examples of Connected Services and Skills., New Connected Services and Skills are added regularly.

- **Connected Microsoft services.** If you choose to connect Cortana to your [Xbox Live](#) account, Cortana can access your Xbox Live data in order to learn about your gaming activity and provide you with relevant content and suggestions, notify you when your friends are available to play, and help you schedule game sessions. If you choose to connect Cortana to your work or school account, Cortana can access data stored in [Office 365](#) to help you stay up to date and get insights about your meetings and relationships. Choosing to sign into LinkedIn within Cortana allows Microsoft to access your LinkedIn data so that Cortana can give you more personalized information and recommendations. Note, Cortana enables LinkedIn to access the name, email address, job title, and company name of people are you are meeting with, in order for Cortana to retrieve relevant information about those contacts.
- **Other Connected services and Skills.** Cortana allows you to connect to third-party services to enable her to do more and provide additional personalized experiences based upon data from the third-party service. Not all Skills require your authentication. With your permission, ***Cortana can also send information about you along with your request to a third-party.*** For instance, Cortana will send your request, along with your current location and destination, to Uber when you ask Cortana to request a ride. You can manage Cortana's Connected Services and Skills in the Cortana Notebook.

When you provide Cortana with permission to access your information from a device or service, this information may be used to seamlessly personalize your Cortana experience on any device or service on which you have enabled Cortana. Remember that you can always sign out of Cortana. When you sign out on Windows, Cortana will still be there to help, but your experiences will not be personalized. You can manage what data Cortana uses, and what it knows about you in Cortana Settings, Permissions, and Notebook. More about the individual features, and how to manage them can be found at go.microsoft.com/fwlink/?linkid=522360.

Groove Music/Movies & TV

Groove Music lets you easily play your music collection, make playlists, buy music and stream custom radio stations. Microsoft Movies & TV allows you to play your video collection, and rent or buy movies and TV episodes. These services were formerly offered as Xbox Music and Video.

To help you discover content that may interest you, Microsoft will collect data about what content you play, the length of play, and the rating you give it. If you sign into Cortana on your device, Microsoft will collect and use data related to the music you play via Groove Music to provide personalized experiences and relevant suggestions.

To enrich your experience when playing content, Groove Music and Movies & TV will display related information about the content you play and the content in your music and video libraries, such as the album title, cover art, song or video title, and other information, where available. To provide this information, Groove Music and Movies & TV send an information request to Microsoft containing standard device data, such as your device IP address, device software version, your regional and language settings, and an identifier for the content.

If you use Groove Music or Movies & TV to access content that has been protected with Microsoft Digital Rights Management (DRM), it may automatically request media usage rights from an online rights server and download and install DRM updates in order to let you play the content. See the DRM information in the [Silverlight](#) section of this privacy statement for more information.

Microsoft Cognitive Services

Microsoft Cognitive Services help developers build apps that can better comprehend data, such as by detecting faces and objects in images, understanding spoken words, or interpreting commands. We collect and use your data to provide the services, which includes improving and personalizing your experiences.

Cognitive Services collect and use many types of data, such as images, audio files, video files, or text, all of which are retained by Microsoft. Microsoft has implemented business and technical measures designed to help de-identify some data Cognitive Services retain. De-identification will not anonymize data completely; for example, a person in a photograph could still be recognized by someone who knows that person.

Microsoft and apps that use Cognitive Services may also collect and use your data. For example, Bing uses search queries collected through the Cognitive Services Bing Search APIs as described in the Bing section. Microsoft Translator uses data sent through the Cognitive Services Translator API as described in the Translator section.

Microsoft Health Services

Microsoft Health services can help you understand and manage your health data. They include HealthVault, HealthVault Insights, Microsoft Band devices, other Microsoft Health applications and related products. The Band helps you keep track of data like heart rate and steps taken. The Band can also use Cortana to take notes and receive notifications from your phone. The Microsoft Health applications send data to Microsoft's servers and allow you to view, manage and control the data. The applications may enable notifications to the Band and other devices. HealthVault services let you gather, edit, add to, and store health data online, along with share your health data with family, caregivers, and health care professionals.

Microsoft Health services collect and use your data to provide the services, which includes improving and personalizing your experiences. Health data you provide to Microsoft through Microsoft Health services is not combined with data from other Microsoft services, or used for other purposes without

your explicit consent. For example, Microsoft does not use your health record data to market or advertise to you without your opt-in consent.

Health Services

Microsoft Health services can help you understand and manage your health data. The data collected depends on the services and features you use, and includes the following:

- **Profile Data.** When you create a profile, you will need to provide data, such as height, weight, and age that is used to calculate your activity results. Other profile data comes from your personal [Microsoft account](#).
- **Activity and Fitness Data.** Microsoft Health services help you keep track of your activity and fitness by collecting data like your heart rate, steps, calories burned, and sleep. Examples of types of activities you can choose to track are runs, workouts, and sleep.
- **Usage Data.** To provide you the best service, we collect and automatically upload statistics about the performance and your use of the Microsoft Health services.
- **Location.** Microsoft Band has built-in Global Positioning System (GPS) capabilities, which let you map your activities like running or biking, without having to carry your phone with you. If you enable GPS for an activity, you can view the activity map in the Microsoft Health applications. Some modes on the Band, such as Golf and Explorer, automatically turn on GPS, and turn it off when you end the mode.

To learn more about the Band's sensors and the data they collect, go [here](#).

Access and Control. You can view and manage your data in Microsoft Health services. For example, you can view and update your profile data, manage connected applications, and view past activities. You can delete specific activity details in the Microsoft Health services. When you delete a specific activity, the event is deleted from the Microsoft Health services; however, other data and the basic sensor data captured by the devices remain in the Microsoft Health services. You can cancel your Microsoft Health services account at any time by contacting Customer Support [here](#).

Cortana. The Microsoft Health services allow you to use Cortana. When you use Cortana, data you process in the Microsoft Health services, including health-related data and data processed from third-party services, is shared with Cortana. Cortana's capabilities allow you to perform queries and set reminders with your voice, if [Cortana](#) is enabled on your device. To learn more about how [Cortana](#) manages your data, see the Cortana section of this privacy statement.

HealthVault

HealthVault is a personal health platform that lets you gather, edit, store, and share health data online. With HealthVault, you can control your own health records. You can also choose to share your health data with family, caregivers, health care professionals, mobile applications, health-related devices, and online tools. For more information about HealthVault, go to [here](#).

Signing into HealthVault. To sign into HealthVault, you can use [Microsoft account](#) or third-party authentication services. If you close your Microsoft account or lose your account credentials, you may not be able to access your data. You can use more than one credential with HealthVault to help ensure continued access. Before using a third-party authentication service with HealthVault, we recommend you review the security and privacy commitments offered by the issuer.

HealthVault Account and Health Records. To create a new HealthVault account, you must provide personal data such as name, date of birth, e-mail address, postal code and country/region. Depending on which features you use, you may be asked for additional information. A HealthVault account allows you to manage one or more health records, such as the ones you create for yourself and your family members. You can add or remove data to a health record you manage at any time.

In the U.S., HealthVault assigns each health record a unique HealthVault email address. When a message is received at that email address, the message and attachments are automatically added to the HealthVault record, and a notification email is sent to the custodians of that record. The email service in HealthVault uses "Direct," a protocol designed specifically to communicate with health care providers. For that reason, HealthVault email can only be sent and received with providers that use a system that uses the Direct protocol. Custodians can add or disable record email addresses.

Sharing Health Data. A key value of HealthVault is the ability you have to share your health data with people and services that can help you meet your health-related goals. By default, you are the custodian of any records you create. Custodians have the highest level of access to a health record. As a custodian, you can share data in a health record with another person by sending an e-mail invitation through HealthVault. You can specify what type of access they have (including custodian access), how long they have access, and whether they can modify the data in the record. When you grant someone access, that person can grant the same level of access to someone else (for example, someone with view-only access can grant another user view-only access). **Because inappropriate granting of access could allow someone to violate your privacy or even revoke your access to your own records, you should be cautious about granting access to your records.**

You can choose to share specific data (or all of the data) in a health record with other services, including participating third-party services you authorize. No service has access to your data through HealthVault unless an authorized user grants it access through HealthVault. HealthVault allows you to control access by accepting or denying requests. For each service granted access, you choose what health information in a specific health record to share and what actions each service may perform on the health information.

A service you authorize for a record will get the full name associated with your HealthVault account, the nickname of the authorized record(s), and your relationship to that record. The service will continue to have access through HealthVault until you revoke the permission. Microsoft can revoke a service's access to HealthVault if it does not meet its privacy commitments to Microsoft. However, except for restricting the access they have to your HealthVault data, we do not control or monitor third-party services, and their privacy practices will vary.

Reports to U.S. Health Care Providers. In the United States, we enable participating health care providers to obtain reports about whether the information they send to a record in Microsoft Health services is used. This feature supports the "meaningful use" objective of the HITECH Act, which provides incentives for health care providers to send their patients copies of their medical information electronically. Providers that participate can get reports that include a number the provider uses to identify the patient within its system, and whether the user took one of the "qualifying actions" in HealthVault (but no information about which action). "Qualifying action" currently includes activities such as viewing, downloading, or transmitting health information via email. You can turn off reporting for your records.

Access and controls. You can review, edit or delete your HealthVault account data, or close your HealthVault account at any time. Only custodians can permanently delete an item. When you delete a health record, it is deleted from all users who had access to it.

When you close your HealthVault account, we delete all records for which you are the sole custodian. If you share custodian access for a record, you can decide whether to delete the record. Microsoft will wait a limited amount of time before permanently deleting your data in order to help avoid accidental or malicious removal of your health data.

HealthVault maintains a full history of each access, change or deletion by users and services, which includes the date, action and name of the person or service. Custodians of records can examine the history of those records.

Email Communications. We will use the email address you provide when you create your HealthVault account to send you an email requesting that you validate your email address, to include in sharing invitations you send through HealthVault, and to send you service notifications, such as email notifications that information is available to add to your HealthVault records.

HealthVault periodically sends newsletters to help keep you informed of the latest improvements. HealthVault will also periodically send you an email summarizing recent account activity. Subject to your contact preferences, we also use your email addresses to send you promotional email. You can unsubscribe from these emails at any time.

Microsoft Translator

Microsoft Translator is a statistical machine translation system designed to automatically translate text and speech between numerous supported languages. Translator may be incorporated into other Microsoft products and services, such as Office, SharePoint, and Bing. Third parties may also incorporate Translator into their own services and offerings. For information on the privacy practices of third-parties' services and offerings, consult their privacy statements.

Microsoft Translator collects and uses the text, image, and speech data you submit, as well as information about how you are accessing the Translator service, such as operating system version, browser type and language. We use your data to provide the Translator service, which includes improving and personalizing your experiences. Microsoft has implemented business and technical measures designed to help de-identify the data Translator retains. For example, we randomly sample text to improve Translator and mask or delete strings of numbers and other personally identifiable information we detect in the sample.

If you subscribe to the Microsoft Translator API with a monthly volume of 250 million characters or more, you may request to have logging turned off for the text you submit to Microsoft Translator by submitting a request using the process detailed at www.microsoft.com/en-us/translator/notrace.aspx.

MSN

MSN services include websites and a suite of apps, including MSN News, Weather, Sports, and Money, and previous versions of the apps branded as Bing (together, "MSN Apps"). The MSN Apps are available on various platforms, including Windows, iOS, and Android. MSN services are also included within other Microsoft services, including the Microsoft Edge browser.

When you install MSN Apps, we collect data that tells us if the app was installed properly, the installation date, the app version, and other data about your device such as the operating system and browser. This data is collected on a regular basis to help us determine the number of MSN App users and identify performance issues associated with different app versions, operating systems, and browsers.

We also collect data about how you interact with MSN services, such as usage frequency and articles viewed, to provide you with relevant content. Some MSN services provide an enhanced experience when you sign in with your Microsoft account, including allowing you to customize your interests and favorites. You can manage personalization through MSN and Bing settings, as well as through settings in other Microsoft services that include MSN services. We also use the data we collect to provide you with advertisements that may be of interest to you. You can opt out of interest-based advertising through the advertising links within MSN services, or by visiting Microsoft's [opt-out page](#).

Previous versions of MSN Money allow you to access personal finance information from third-party financial institutions. MSN Money only displays this information and does not store it on our servers. Your log-in credentials used to access your financial information from third parties are encrypted on your device and are not sent to Microsoft. These financial institutions, as well as any other third-party services you access through MSN services, are subject to their own terms and privacy policies.

Office

Office is a collection of productivity applications including Word, Excel, PowerPoint, and Outlook among others. For more details about Outlook, see the [Outlook](#) section of this privacy statement. Various Office applications enable you to use content and functionality from other Microsoft services, such as Bing, and third-party connected services. For detailed information about how to manage your privacy options, please see go.microsoft.com/fwlink/?LinkId=624445. If you work in an organization, your administrator can turn off connected services via Group Policy.

Office Roaming Service. The Office Roaming Service helps keep your Office settings up-to-date across your devices running Office. When you sign into Office with your [Microsoft account](#), the Office Roaming Service is turned on and syncs some of your customized Office settings to Microsoft servers (such as a list of most recently used documents and the last location viewed within a document). When you sign into Office on another device with the same account, the Office Roaming Service downloads your settings from Microsoft servers and applies them to the additional device. The Office Roaming Service also applies some of your customized Office settings when you sign into Office.com. When you sign out of Office, the Office Roaming Service removes your Office settings

from your device. Any changes you made to your customized Office settings are sent to Microsoft servers.

Microsoft Updates. Office uses the [Microsoft Update](#) service to provide you with security and other important updates. See the Update Services section of this privacy statement for more information.

Online Help, templates, fonts, and other content. Office uses other Microsoft or third-party services to give you the latest online content when you are connected to the Internet such as Help articles, templates, and fonts. For example, when you use the Help feature in Office applications, Office sends your search query to Office.com to provide you with online Help articles. These features are turned on by default, but you can turn them off using privacy settings. You can access privacy settings in Office 2013 by clicking **File > Options > Trust Center > Trust Center Settings > Privacy Options**.

Click-to-Run Update Service. The Click-to-Run Update Service allows you to install certain Microsoft Office products over the Internet, so you can start using them before they are completely downloaded. By default, the Click-to-Run Update Service also automatically detects online updates to Click-to-Run-enabled products on your device and downloads and installs them automatically. The service is turned on by default, but you can turn it off by using privacy settings.

Search services. Office-supported search services such as Insights allow you to request information from Microsoft or third-party services from within an Office application. For example, in Word, you can highlight a word or phrase and retrieve relevant information from Bing search. When you search on a particular word or phrase, Office sends to the service the encrypted text you requested (and when using Insights, in order to provide you with contextually relevant search results, Office will send your requested word or phrase and some surrounding content from your document). In Excel, you can send categories of data to Microsoft in order to receive recommendations for other sets of similar data that might interest you, but the actual content from your workbook isn't sent to Microsoft. In addition, Office will send data about the software you're using and the locale to which your system is set. If required by a third-party content provider, it will also send authorization data indicating you have the right to download the relevant content. Frequently, the information you receive includes a link to additional information from the content provider's website. If you click the link, the content provider may place a [cookie](#) on your device to identify you for future transactions.

Translation service. Some Office applications allow you to translate some or all of your document by using a bilingual dictionary or a machine translation. If a word or phrase you want to translate isn't in the bilingual dictionary included with your application software, the word or phrase is sent unencrypted to a Microsoft or a third-party translation service. If you choose to translate your entire document, the entire document is sent unencrypted to a Microsoft or a third-party translation service. In addition to the word or phrase you want to translate, Office sends information about the Office software you are using, including the version, operating system, and locale and language to which your system is set. For third-party translation services, Office might also send previously stored authentication information indicating that you previously signed up for access to the website.

OneDrive

OneDrive lets you store and access your files on virtually any device. You can also share and collaborate on your files with others. Some versions of the OneDrive application enable you to access both your personal OneDrive by signing in with your personal Microsoft account and your OneDrive

for Business by signing in with your work or school Microsoft account as part of your organization's use of Office 365.

When you use OneDrive, we collect data about your usage of the service, as well as the content you store in order to provide, improve and protect the services. Examples include, indexing the contents of your OneDrive documents so that you can search for them later and using location information to enable you to search for photos based on where the photo was taken. We also collect device information so we can deliver personalized experiences, such as enabling you to sync content across devices and roam customized settings.

When you store content in OneDrive, that content will inherit the sharing permissions of the folder in which you store it. For example, if you store content in the public folder, the content will be public and available to anyone on the Internet who can find the folder. If you store content in a private folder, the content will be private.

When you share content to a social network like Facebook from a phone that you have synced with your OneDrive account, your content is either uploaded to that network or a link to that content is posted to that network. Content posted to social networks and hosted on OneDrive is accessible to anyone on that social network. To delete the content, you need to delete it from the social network and from OneDrive.

When you share your OneDrive content with your friends via a link, an email with the link is sent to those friends. The link contains an authorization code that allows anyone with the link to access your content. If one of your friends sends the link to other people, they will also be able to access your content, even if you did not choose to share the content with them. To revoke permissions for your content on OneDrive, sign into your account and then select the specific content to manage the permission levels. Revoking permissions for a link effectively deactivates the link. No one will be able to use the link to access the content unless you decide to share the link again.

Files managed with OneDrive for Business are stored separately from files stored with your personal OneDrive. OneDrive for Business collects and transmits personal data for authentication, such as your email address and password, which will be transmitted to Microsoft and/or to the provider of your Office 365 service.

Outlook

Outlook products are designed to improve your productivity through improved communications and include Outlook.com, Outlook applications, and related services.

Outlook.com. Outlook.com is Microsoft's primary consumer email service, and includes email accounts with addresses that end in outlook.com, live.com, hotmail.com, and msn.com. Outlook.com provides features that let you connect with your friends on social networks. You will need to create a [Microsoft account](#) to use Outlook.com.

When you delete an email or item from a mailbox in Outlook.com, the item generally goes into your Deleted Items folder where it remains for approximately 7 days unless you move it back to your inbox, you empty the folder, or the service empties the folder automatically, whichever comes first. When the Deleted Items folder is emptied, those emptied items remain in our system for up to 30 days before final deletion.

Outlook Applications. Outlook client applications are software you install on your device that permits you to manage email, calendar items, files, contacts, and other data from email, file storage, and other services, like Exchange Online or Outlook.com, or servers, like Microsoft Exchange. You can use multiple accounts from different providers, including third-party providers, with Outlook applications.

To add an account, you must provide permission for Outlook to access data from the email or file storage services.

When you add an account to Outlook, your mail, calendar items, files, contacts, settings and other data from that account will automatically sync to your device. If you are using the mobile Outlook application, that data will also sync to Microsoft servers to enable additional features such as, faster search, personalized filtering of less important mail, and an ability add email attachments from linked file storage providers without leaving the Outlook application. If you are using the desktop Outlook application, you can choose whether to allow the data to sync to our servers. At any time, you can remove an account or make changes to the data that is synced from your account.

If you add an account provided by an organization (such as your employer or school), the owner of the organizational domain can implement policies and controls (for example, requiring multi-factor authentication or the ability to remotely wipe data from your device) that can affect your use of Outlook.

To learn more about the data the Outlook applications collect and process, please see the [Office](#) section of this privacy statement.

Silverlight

Microsoft Silverlight helps you to access and enjoy rich content on the Web. Silverlight enables websites and services to store data on your device. Other Silverlight features involve connecting to Microsoft to obtain updates, or to Microsoft or third-party servers to play protected digital content.

Silverlight Configuration tool. You can make choices about these features in the Silverlight Configuration tool. To access the Silverlight Configuration tool, right click on content that is currently being displayed by Silverlight and select **Silverlight**. You can also run the Silverlight Configuration tool directly. In Windows, for example, you can access the tool by searching for "Microsoft Silverlight."

Silverlight application storage. Silverlight-based applications can store data files locally on your computer for a variety of purposes, including saving your custom settings, storing large files for graphically intensive features (such as games, maps, and images), and storing content that you create within certain applications. You can turn off or configure application storage in the Silverlight Configuration tool.

Silverlight updates. Silverlight will periodically check a Microsoft server for updates to provide you with the latest features and improvements. A small file containing information about the latest Silverlight version will be downloaded to your computer and compared to your currently installed version. If a newer version is available, it will be downloaded and installed on your computer. You can turn off or configure updates in the Silverlight Configuration tool.

Digital Rights Management. Silverlight uses Microsoft Digital Rights Management (DRM) technology to help protect the rights of content owners. If you access DRM-protected content (such as music or video) with Silverlight, it will request media usage rights from a rights server on the Internet. In order to provide a seamless playback experience, you will not be prompted before Silverlight sends the request to the rights server. When requesting media usage rights, Silverlight will provide the rights server with an ID for the DRM-protected content file and basic data about your device, including data about the DRM components on your device such as their revision and security levels, and a unique identifier for your device.

DRM updates. In some cases, accessing DRM-protected content will require an update to Silverlight or to the DRM components on your device. When you attempt to play content that requires a DRM update, Silverlight will send a request to a Microsoft server containing basic data about your device, including information about the DRM components on your computer such as their revision and security levels, troubleshooting data, and a unique identifier for your device. The Microsoft server uses this identifier to return a unique DRM update for your device, which will then be installed by Silverlight. You can turn off or configure DRM component updates on the **Playback** tab in the Silverlight Configuration tool.

Skype

Skype lets you send and receive voice, video and instant message communications. This section applies to the consumer version of Skype; if you are using Skype for Business, see the [Enterprise Products](#) section of this privacy statement. Both Microsoft Corporation and Skype Communications S.à.r.l. (a wholly-owned Microsoft subsidiary based in Luxembourg) are data controllers for Skype, and references to Microsoft in this section refer to both legal entities.

As part of providing these features, Microsoft collects usage data about your communications that includes the time and date of the communication and the numbers or usernames that are part of the communication.

Skype profile. To enable other people to find you on Skype (or products that interact with Skype, such as Skype for Business), depending on your profile settings, your Skype profile is included in the search directory. Your profile includes your username, avatar, and any other data you choose to add to your profile or display to others.

Skype Contacts. If you use a Microsoft service, such as Outlook.com, to manage contacts, Skype will automatically add the people you know to your Skype contact list. With your permission, Skype will also check your device or other address books from time to time to automatically add your friends as Skype contacts. You can block users if you don't want to receive their communications.

Partner companies. To make Skype available to more people, we partner with other companies to allow Skype to be offered via those companies' services. If you use Skype through a company other than Microsoft, that company's privacy policy governs how it handles your data. To comply with applicable law or respond to valid legal process, or to help our partner company or local operator comply or respond, we may access, transfer, disclose, and preserve your data. That data could include, for example, your private content, such as the content of your instant messages, stored video messages, voicemails, or file transfers.

Skype Manager. Skype Manager lets you manage a group's (such as your family's) Skype usage from one central place. When you set up a group, you will be the Skype Manager Administrator and

can see the patterns of usage, including detailed information, like traffic data and details of purchases, of other members of the group who have consented to such access. If you add information like your name, other people in the group will be able to see it. Members of the group can withdraw consent for Skype Manager on their account page at www.skype.com.

Skype marketing affiliate program. So that more people can learn about Skype, we encourage other companies and organizations to sign up as marketing affiliates to refer people to Skype. When the people they refer do things like buy Skype Credit, we pay them. We partner with another company, Conversant Media, to operate our affiliate network. Microsoft, our network partner, and the marketing affiliates use cookies and web beacons so we can know which marketing affiliate made a successful referral and earned a payment. Microsoft doesn't control the cookies that the marketing affiliates set. For more information on the privacy practices of our network partner, visit www.conversantmedia.com/legal/privacy.

Push notifications. To let you know of incoming calls, chats and other messages, Skype apps use the notification service on your device. For many devices, these services are provided by a another company. To tell you who is calling, for example, or to give you the first few words of the new chat, Skype has to tell the notification service so that they can provide the notification to you. The company providing the notification service on your device will use this information in accordance with their own terms and privacy policy. Microsoft is not responsible for the data collected by company providing the notification service. If you don't want to use the notification services for incoming Skype calls and messages, turn it off in the settings found in the Skype application or your device.

Skype advertising. Some Skype software includes interest-based advertising, so that you're more likely to see ads you'll like. In some versions of the software, you can opt out of interest-based advertising in the privacy options or account settings menu. If you sign in to Skype with a Microsoft account, you can opt out of interest-based advertising at choice.microsoft.com. If you opt out, you'll still see ads displayed in the Skype software based on your country of residence, language preference, and IP address location, but other data is not used for ad targeting.

Translation features. To help you communicate with people in different languages, some Skype apps offer audio and/or text translation features. When you use translation features, your voice and text data are used to provide and improve Microsoft speech recognition and translation services.

Recording features. Some versions of Skype have a recording feature that allows you to capture and share audio and/or video clips of your conversation. If you choose to record a session, the recording may include a few seconds of the call held in memory prior to your initiating the recording. The recording will be stored as part of your conversation history and may also be stored locally on your device. ***You should understand your legal responsibilities before recording any communication. This includes whether you need to get consent from all parties to the communication in advance.*** Microsoft is not responsible for how you use your recordings or the recording features.

Store

The Store is an online service that allows you to browse, download, purchase, rate, and review applications and other digital content. It includes:

- Windows Store for apps and content for Windows devices such as phones, PCs, and tablets,
- Xbox Store for games and other apps for Xbox ONE and Xbox 360 consoles, and

- Office Store for products and apps for Office, SharePoint, Exchange, Access and Project (2013 versions or later).

We collect data about how you access and use the Store; the products you've viewed, purchased, or installed; the preferences you set for viewing apps in the Store; and any ratings, reviews or problem reports you submit. Your Microsoft account is associated with your ratings and reviews; and if you write a review, the name and picture from your Microsoft account will be published with your review.

Permission for Store apps. Many apps you install from the Windows Store are designed to take advantage of specific hardware and software features of your device. An app's use of certain hardware and software features may give the app or its related service access to your data. For example, a photo editing app might access your device's camera to let you take a new photo or access photos or videos stored on your device for editing, and a restaurant guide might use your location to provide nearby recommendations. Information about the features that an app uses is provided on the app's product description page in the Store. Many of the features that Windows Store apps use can be turned on or off through your device's privacy settings. In Windows, in many cases, you can choose which apps can use a particular feature. Go to **Start > Settings > Privacy**. Select the feature (for example, Calendar) and select which app permissions are on or off. The lists of apps in Windows privacy settings that can use hardware and software features will not include "Classic Windows" applications, and these applications are not affected by these settings.

App updates. Unless you have turned off automatic app updates in the relevant Store settings, the Store will automatically check for, download, and install app updates to ensure that you have the latest versions. Updated apps might use different Windows hardware and software features from the previous versions, which could give them access to different data on your device. You will be prompted for consent if an updated app accesses certain features, such as location. You can also review the hardware and software features an app uses by viewing its product description page in the Windows Store.

Each app's use of your data collected through any of these features is subject to the app developer's privacy policies. If an app available through the Windows Store collects and uses any of your personal data, the app developer is required to provide a privacy policy, and a link to the privacy policy is available on the app's product description page in the Store.

Sideloaded apps and developer mode. Developer features such as the "developer mode" setting are intended for development use only. If you enable developer features, your device may become unreliable or unusable, and expose you to security risks. Downloading or otherwise acquiring apps from sources other than the Store, also known as "sideloading" apps, may make your device and personal data more vulnerable to attack or unexpected use by apps. Windows policies, notifications, permissions and other features intended to help protect your privacy when apps access your data may not function as described in this statement for sideloaded apps or when developer features are enabled.

SwiftKey

SwiftKey Keyboard and related apps and services use data about how you type – including the emoji you use and the words that matter to you – to learn your writing style and provide personalized autocorrect and predictive text that adapts to you.

When you use our products, we collect data such as device, network, performance, and usage statistics. We use this data to operate and improve the products.

If you opt in to SwiftKey Cloud, we will collect your email address, basic demographic data, and data about the words and phrases you use to enable services such as personalization, prediction synchronization, and backup. Our prediction technology learns from the way you use language to build a personalized language model. This model is an optimized view of the words and phrases that you use most often, and reflects your unique writing style. To do this, the SwiftKey Keyboard for Android accesses your SMS messages upon first installation. The SwiftKey personalization service, which is a feature of SwiftKey Cloud, also accesses your recent content from online services that you specify, such as Gmail, Facebook and Twitter. If you are logged into SwiftKey Cloud, this data will be transferred over encrypted channels to our servers. Where a field has been flagged by a website or app as denoting a password field or payment data, SwiftKey does not log, store, or learn from this data.

If you are not logged into SwiftKey Cloud, language insights will not be collected from your device. You may at any time withdraw your consent for our use and retention of personal data collected by SwiftKey by going to the SwiftKey Cloud section in SwiftKey Settings. By withdrawing consent, your personal data collected through your use of the SwiftKey Keyboard will be deleted.

You may receive occasional notifications on your device alerting you to product updates and features that may be of interest to you. You can disable these notifications in our products at any time by going to the SwiftKey Settings.

Windows

Windows is a personalized computing environment that enables you to seamlessly roam and access services, preferences and content across your computing devices from phones to tablets to the Surface Hub. Rather than residing as a static software program on your device, key components of Windows are cloud-based, and both cloud and local elements of Windows are updated regularly, providing you with the latest improvements and features. In order to provide this computing experience, we collect data about you, your device, and the way you use Windows. And because Windows is personal to you, we give you choices about the personal data we collect and how we use it. Note that if your Windows device is managed by your organization (such as your employer or school), your organization may use centralized management tools provided by Microsoft or others to control device settings, device policies, software updates, data collection by us or the organization, or other aspects of your device. For more information about data collection and privacy in Windows, go to go.microsoft.com/fwlink/?LinkId=529552. Legacy versions of Windows (including Vista, 7, 8, and 8.1) are subject to their own privacy statements.

Activation

When you activate Windows, a specific product key is associated with the device on which your software is installed. The product key and data about the software and your device is sent to Microsoft to help validate your license to the software. This data may be sent again if there is a need to re-activate or validate your license. On phones running Windows, device and network identifiers, as well as device location at the time of the first power up of the device, are also sent to Microsoft for the purpose of warranty registration, stock replenishment, and fraud prevention.

Advertising ID

Windows generates a unique advertising ID for each user on a device. When the advertising ID is enabled, apps (both Microsoft apps and third-party apps) can access and use the advertising ID in much the same way that websites can access and use a unique identifier stored in a cookie. Thus, your advertising ID can be used by app developers and advertising networks to provide more relevant advertising and other personalized experiences across their apps and on the web. Microsoft collects the advertising ID for the uses described here only when you choose to enable the advertising ID as part of your privacy setting. You can turn off access to this identifier at any time by turning off the advertising ID in your privacy settings (in Start > Settings > Privacy). If you choose to turn it on again, the advertising ID will be reset and a new identifier will be generated. When a third-party app accesses the advertising ID, its use of the advertising ID will be subject to its own privacy policy. For more information on Microsoft's use of data for advertising, see the [How We Use Data](#) section of this statement.

Diagnostics

As you use Windows, we collect diagnostic data that helps us fix problems and improve Microsoft products. If you choose to turn on **Tailored experiences**, this data can also be used to personalize your experiences with Microsoft products. This data is transmitted to Microsoft and stored with one or more unique identifiers that can help us recognize an individual user on an individual device and understand the device's service issues and use patterns. There are two levels of diagnostic and usage data: **Basic** and **Full**. At the lowest level, **Basic**, we collect only data necessary to keep Windows devices up-to-date and secure. Basic data includes data about the device itself, the proper functioning of Windows and Store updates, and basic error data. We collect the following data at the Basic level:

- Device, connectivity and configuration data:
 - Data about the device such as the processor type, OEM manufacturer, type of battery and capacity, number and type of cameras, firmware, and memory attributes.
 - Network capabilities and connection data such as the device's IP address, mobile network (including IMEI and mobile operator) and whether the device is connected to a free or paid network.
 - Data about the operating system and its configuration such as the OS version and build number, region and language settings, diagnostics level, and whether the device is part of the Windows Insider program.
 - Data about connected peripherals such as model, manufacturer, drivers, and compatibility data.
 - Data about the applications installed on the device such as application name, version, and publisher.
- Whether a device is ready for an update and whether there are factors that may impede the ability to receive updates, such as low battery, limited disk space, or connectivity through a paid network.
- Whether updates complete successfully or fail.
- Data about the reliability of the diagnostics collection system itself.

- Basic error reporting, which is health data about the operating system and applications running on your device. For example, basic error reporting tells us if an application, such as Microsoft Paint or a third-party game, hangs or crashes.

For more information about what is collected in Basic data, click [here](#) (English only).

Full data includes everything collected with Basic data, plus additional information that enables Microsoft to fix and improve products and services for all users. We collect the following additional information at the Full level:

- Additional data about the device, connectivity and configuration, beyond that collected at Basic.
- Status and logging information about the health of operating system and other system components (in addition to data about the update and diagnostics systems collected at Basic).
- App usage, such as which programs are launched on a device, how long they run, and how quickly they respond to input.
- Browser usage, including browsing history and search terms, on Microsoft browsers, such as Microsoft Edge or Internet Explorer.
- Small samples of inking and typing input, which is processed to remove identifiers, sequencing information, and other data (such as names, email addresses, and numeric values) which could be used to reconstruct the original content or associate the input to the user. This data is never used for Tailored experiences as described below.
- Enhanced error reporting, including the memory state of the device when a system or app crash occurs (which may unintentionally contain user content, such as parts of a file you were using when the problem occurred). Crash data is never used for Tailored experiences as described below.

We provide limited portions of error report information to partners (such as OEMs) to help them troubleshoot products and services which work with Windows and other Microsoft product and services. They are only permitted to use this information to repair or improve those products and services.

If you choose to turn on **Tailored experiences**, we will use some of the data described above in Diagnostics to personalize your experiences with Windows and other products and services. This includes suggestions on how to customize and optimize Windows; and recommendations and offers of Windows features and supported apps, services, hardware, and peripherals. The scope of data will depend on whether you choose Full or Basic as your Diagnostics setting. For example, if you choose Full, your data will include browser and app usage. However, even if you enable Tailored experiences, we will not use your crash, typing, or inking input data for personalization.

Location Services, Motion Sensing, & Recording

Windows location service. Microsoft operates a location service that helps determine the precise geographic location of a specific Windows device. Depending on the capabilities of the device, location is determined using satellite global positioning service (GPS), detecting nearby cell towers and/or Wi-Fi access points and comparing that information against a database that Microsoft maintains of cell towers and Wi-Fi access points whose location is

known, or deriving location from your IP address. When the location service is active on a Windows device, or you have given permission for Microsoft apps to access location information on non-Windows devices, data about cell towers and Wi-Fi access points and their locations is collected by Microsoft and added to the location database after removing any data identifying the person or device from which it was collected. Microsoft may also share this de-identified location data with third parties to provide and improve location and mapping services.

Windows services and features (such as browsers and Cortana), applications running on Windows, and websites opened in Windows browsers can access the Windows location service to determine precise location if you allow them to do so. Some features and apps request precise location permission when you first install Windows, some ask the first time you use the app, and others ask every time you access the location service. For information about certain Windows apps that use the location service, see the [Windows Apps](#) section below.

When the location service is accessed, your Windows device will also upload its location to Microsoft, and we will retain only the last known location (each new location replaces the previous one) to improve the efficiency and operation of our services. Data about a Windows device's recent location history is stored on the device, and certain apps and Windows features can access this location history. You can clear your device's location history at any time in the device's Settings menu.

In Settings, you can also view which applications have access to the location service or your device's location history, turn off or on access to the location service for particular applications, or turn off the location service. You can also set a default location, which will be used when the location service can't detect a more exact location for your device.

Note that on mobile devices, your mobile operator will have access to your location even if you turn off the location service.

General Location. If you turn on the General Location feature, apps that cannot use your precise location will have access to your general location, such as your city, postal code, or region.

Find My Phone. The Find My Phone feature allows you to find the location of your Windows phone from account.microsoft.com, even if you have turned off all access to the location service on the phone. If you have turned on the "save my location every few hours" feature in the Find My Phone settings on your phone, the Find My Phone feature will periodically send and store a single last known location of your phone, even if you have turned off location services on your phone. Each time a new location is sent, it replaces the previously-stored location.

Find My Device. The Find My Device feature allows an administrator of a Windows PC or tablet to find the location of that device if the administrator has enabled the location service for the device, even if other users have disabled location for themselves. When the administrator attempts to locate the device, users will see a notification in the notification center.

Windows Motion Sensing. Windows devices with motion activity detection can collect motion activity. This data can enable features such as a pedometer to count the number of steps you take, so a fitness application can estimate how many calories you burn. This data and history is stored on your device and can be accessed by applications you give permission to access and use that data.

Recording. Some Windows devices have a recording feature that allows you to capture audio and video clips of your activity on the device, including your communications with others. If you choose to record a session, the recording will be saved locally on your device. In some cases, you may have the option to transmit the recording to a Microsoft product or service that broadcasts the recording publicly. **IMPORTANT: You should understand your legal responsibilities before recording and/or transmitting any communication. This includes whether you need to get consent from all parties to the communication in advance.** Microsoft is not responsible for how you use recording features or your recordings.

Security and Safety Features

Device encryption. Device encryption helps protect the data stored on your device by encrypting it using BitLocker Drive Encryption technology. When device encryption is on, Windows automatically encrypts the drive Windows is installed on and generates a recovery key. The BitLocker recovery key for your personal device is automatically backed up online in your personal Microsoft OneDrive account. Microsoft doesn't use your individual recovery keys for any purpose.

Malicious Software Removal Tool. The Malicious Software Removal Tool (MSRT) runs on your device at least once per month as part of Windows Update. MSRT checks devices for infections by specific, prevalent malicious software ("malware") and helps remove any infections found. When the MSRT runs, it will remove the malware listed on the Microsoft Support website if the malware is on your device. During a malware check, a report will be sent to Microsoft with specific data about malware detected, errors, and other data about your device. If you do not want MSRT to send this data to Microsoft, you can disable MSRT's reporting component.

Microsoft Family. Parents can use Microsoft Family to understand and set boundaries on how their child is using their device. There are many features available to Family members, so please carefully review the information provided when you create or join a Family. When Family activity reporting is turned on for a child, Microsoft will collect details about how the child uses their device and provide parents with reports of that child's activities. Activity reports are routinely deleted from Microsoft servers after a short period of time.

SmartScreen. SmartScreen helps protect you when using our services by checking downloaded files and web content for malicious software, potentially unsafe web content, and other threats to you or your device. When checking a file, data about that file is sent to Microsoft, including the file name, a hash of the file's contents, the download location, and the file's digital certificates. If SmartScreen identifies the file as unknown or potentially unsafe, you will see a warning prior to opening the file. When checking web content, data about the content and your device is sent to Microsoft, including the full web address of the content. If SmartScreen detects that content is potentially unsafe, you will see a warning in place of the content. SmartScreen can be turned on or off in Settings.

Windows Defender. Windows Defender looks for malware and other unwanted software on your device. Windows Defender is automatically turned on to help protect your device if no other antimalware software is actively protecting your device. If Windows Defender is turned on, it will monitor the security status of your device. When Windows Defender is turned on, or is running because Limited Periodic Scanning is enabled, it will automatically send reports to Microsoft that contain data about suspected malware and other unwanted software, and it may also send files that could contain malware. If a report is likely to contain personal data, the report is not sent automatically, and you'll be prompted before it is sent. You can configure Windows Defender not to send reports and suspected malware to Microsoft.

Speech, Inking and Typing

Windows provides both a device based speech recognition feature (available through the Windows Speech Recognition Desktop app), and a cloud-based speech recognition service that was introduced alongside Cortana in those markets and regions where Cortana is available. Go here support.microsoft.com/instantanswers/557b5e0e-0eb0-44db-87d6-5e5db6f9c5b0/cortana-s-regions-and-languages to learn what languages and regions speech currently supports. When you use cloud-based speech recognition, Microsoft collects and uses your voice input to provide you with speech recognition services in Cortana and other supported applications.

Additionally, your typed and handwritten words are collected to provide you a personalized user dictionary, help you type and write on your device with better character recognition, and provide you with text suggestions as you type or write. Typing data includes a sample of characters and words you type, which we scrub to remove IDs, IP addresses, and other potential identifiers. It also includes associated performance data, such as changes you manually make to text, as well as words you've added to the dictionary.

As part of the cloud-based speech recognition service, we also collect information from the user dictionary created on your device. Both the voice data and the user dictionary are collected and used in the aggregate to help improve our ability to correctly recognize all users' speech.

If you've given permission in Cortana, we also collect your name and nickname, your recent calendar events and the names of the people in your appointments, information about your contacts including names and nicknames, names of your favorite places, apps you use, and information about your music preferences. This additional data enables us to better recognize people, events, places, and music when you dictate commands, messages, or documents.

You can turn cloud speech recognition off at any time. This will stop the data collection for this feature and will delete associated data stored on your device, such as your local user dictionary and your input history.

Sync Settings

When you sign into Windows with a Microsoft account, Windows syncs some of your settings and data with Microsoft servers to make it easier to have personalized experiences across multiple devices. After you've signed into one or more devices with a Microsoft account, when you sign into another with the same Microsoft account for the first time,

Windows will download and apply the settings and data you choose to sync from your other devices. Settings you choose to sync will automatically update on Microsoft servers and your other devices as you use them.

Some of the settings that are synced include:

- Apps you've installed from the Windows Store
- Language preferences
- Ease of Access preferences
- Personalization settings such as your account picture, background, and mouse settings
- Settings for Windows Store apps
- Spell checker dictionaries, input method editor (IME) dictionaries, and personal dictionaries
- Internet Explorer browser history, favorites, and websites you have open
- Saved app, website, mobile hotspot, and Wi-Fi network names and passwords

You can choose whether to sync your settings, and control what is synced, by going to Sync Settings in the Accounts section of Windows Settings. Some apps have their own, separate sync controls. If you sign into Windows with a work account and you choose to connect that account to your personal Microsoft account, Windows will ask which settings you want to sync before connecting your Microsoft account.

Update Services

Update Services for Windows includes Windows Update and Microsoft Update. Windows Update is a service that provides you with software updates for Windows software and other supporting software, such as drivers and firmware supplied by device manufacturers. Microsoft Update is a service that provides you with software updates for other Microsoft software such as [Office](#).

Windows Update automatically downloads Windows software updates to your device. You can configure Windows Update to automatically install these updates as they become available (recommended) or have Windows notify you when a restart is required to finish installing updates. Apps available through the Windows Store are automatically updated through the Store, as described in the [Store](#) section above.

Web Browsers: Microsoft Edge and Internet Explorer

Microsoft Edge is Microsoft's default web browser for Windows. Internet Explorer, Microsoft's legacy browser, is also available in Windows. Whenever you use a web browser to access the Internet, data about your device ("standard device data") is sent to the websites you visit and online services you use. Standard device data includes your device's IP address, browser type and language, access times, and referring website addresses. This data might be logged on those websites' web servers. Which data is logged and how that data is used depends on the privacy practices of the websites you visit and web services you use.

Additionally, data about how you use your browser, such as your browsing history, web form data, temporary Internet files, and [cookies](#), is stored on your device. You can delete this data from your device using Delete Browsing History.

New features in Microsoft Edge allow you to capture and save content on your device, such as:

- **Web Note:** which allows you to create ink and text annotations on the web pages you visit, and clip, save or share them;
- **Active Reading:** which allows you to create and manage reading lists including websites or documents; and
- **Hub:** which allows you to easily manage your reading lists, favorites, downloads, and history all in one area.

Some Microsoft browser information saved on your device will be synced across other devices when you sign in with your Microsoft account. For instance, in Internet Explorer, this information includes your browsing history and favorites; and in Microsoft Edge, it includes your favorites and reading lists. As an example, if you sync your Microsoft Edge reading list across devices, copies of the content you choose to save to your reading list will be sent to each synced device for later viewing. You can disable syncing in Internet Explorer by going to Sync Settings in the Accounts section of Windows Settings (see [Sync Settings](#)). You can also disable syncing of Microsoft Edge browser information by turning off the sync option in Microsoft Edge Settings.

Microsoft Edge and Internet Explorer use your search queries and browsing history to provide you with faster browsing and more relevant search results. These features include:

- **AutoSearch and Search Suggestions** in Internet Explorer automatically sends the information you type into the browser address bar to your default search provider (such as Bing) and offer search recommendations as you type each character. In Microsoft Edge, this feature automatically sends this information to Bing even if you have selected another default search provider.
- **Suggested Sites** recommends web contents that you might be interested in based on your search and browsing history.

Browsing data collected in connection with these features is used in the aggregate and you can turn off any of these features at any time. These features will not collect browsing history while you have InPrivate Browsing enabled.

In order to provide search results, Microsoft Edge and Internet Explorer send your search queries, standard device information, and location (if you have location enabled) to your default search provider. If Bing is your default search provider, we use this data as described in the [Bing](#) section of this privacy statement.

Cortana can assist you with your web browsing in Microsoft Edge with features such as Ask Cortana. You can disable Cortana assistance in Microsoft Edge at any time in Microsoft Edge Settings. To learn more about how Cortana uses data and how you can control that, go to the [Cortana](#) section of this privacy statement.

Wi-Fi Connecting to suggested open hotspots

If you turn it on Connect to suggested open hotspots in Wi-Fi settings, you will automatically connect to suggested open Wi-Fi networks. Please note that not all networks are secure - be

careful using an open network to do something online that requires sensitive or personal data, such as making a banking transaction or a purchase.

Windows Apps

A number of Microsoft apps are included with Windows and others are available in the Windows Store. Some of those apps include:

Maps app. The Maps app provides location-based services and uses Bing services to process your searches within the Maps app. Please see the [Bing](#) section of this privacy statement to learn more about these Bing-powered experiences. When the Maps app has access to your location, even when the app is not in use, Microsoft may collect de-identified location data from your device to improve Microsoft's services. You can disable the Maps app's access to your location by turning off the location service or turning off the Maps app's access to the location service.

You can keep track of your favorite places and recent map searches in the Maps app. Your favorite places and search history will be included as search suggestions. If you're signed in with your Microsoft account, your favorite places, search history, and certain app settings will be synced across other devices and services (for example, Cortana). See [Sync Settings](#) above for more information.

Camera and Photo apps. If you allow the Camera app to use your location, location data is embedded in the photos you take with your device. Other descriptive data, such as camera model and the date that the picture was taken, is also embedded in photos and videos. If you choose to share a photo or video, any embedded data will be accessible to the people and services you share with. You can disable the Camera app's access to your location by turning off all access to the location service in your device's Settings menu or turning off the Camera app's access to the location service.

Your photos, videos, as well as screenshots, saved in your camera roll automatically upload to OneDrive. You can manage your photos and/or videos in OneDrive, and you can disable the automatic upload in Settings.

When you take photos embedded with your location, the Photos app can group your photos by time and location. To group your photos, the Photos app sends location data in your photos to Microsoft to determine the names of locations, such as "Seattle, Washington". When you are using the Photo app while signed into your Microsoft account, your photos and videos from OneDrive will be automatically sorted in into albums in the Photo app, and will also appear on the Photo app's live tile. Your photos and/or videos will only be shared with others if you choose to do so.

People app. The People app lets you see and interact with all your contacts in one place. When you add your Microsoft account to a Windows device, your contacts from your account will be automatically added to the People app. You can add other accounts to the People app, including your social networks (such as Facebook and Twitter) and email accounts. When you add an account, we tell you what data the People app can import or sync with the particular service and let you choose what you want to add. Other apps you install may also sync data to the People app, including providing additional details to existing contacts. You can remove an account from the People app at any time.

Mail and Calendar app. The Mail and Calendar app allows you to connect all your email, calendars, and files in one place, including those from third-party email and file storage providers. The app provides location-based services, such as weather information in your calendar, but you can disable the app's use of your location. When you add an account to the Mail and Calendar app your email, calendar items, files, contacts, and other settings from your account will automatically sync to your device and to Microsoft's servers. At any time, you can remove an account or make changes to the data that's synced from your account. To configure an account, you must provide the app with the account credentials (such as user name and password), which will be sent over the Internet to the third-party provider's server. The app will first attempt to use a secure (SSL) connection to configure your account but will send this information unencrypted if your email provider does not support SSL. If you add an account provided by an organization (such as a company email address), the owner of the organizational domain can implement certain policies and controls (for example, multi-factor authentication or the ability to remotely wipe data from your device) that may affect your use of the app.

Messaging app. When you sign in with a Microsoft account on your device, you can choose to back up your information, which will sync your SMS and MMS messages and store them in your Microsoft account. This allows you to retrieve the messages if you lose or change phones. After your initial device set-up, you can manage your messaging settings at any time. Turning off your SMS/MMS backup will not delete messages that have been previously backed up to your Microsoft account. To delete such messages from storage, you must delete them from your device prior to turning off backup. If you allow the Messaging app to use your location, you can attach a link to your current location to an outgoing message. Location information will be collected by Microsoft as described in the Windows [Location Services](#) section.

Microsoft Wallet App for Windows Phone. You can use Microsoft Wallet to hold information such as coupons, loyalty cards, tickets, and other digital content. Where available, you can also add payment cards to the Microsoft Wallet to make payments at participating stores using NFC (near-field communication).

You can set up your wallet for payment by logging into Microsoft Wallet with your personal Microsoft account and adding payment cards associated with your Microsoft account. When you add a payment card to Microsoft Wallet, we provide data to your bank and payment card network, including your name, card number, billing address, email address, device data (including the device name, type, and identifier), and your location at the time you add your payment card to your wallet. This data is sent to your bank and payment card network to determine the eligibility of your payment card, enable transactions, detect fraud.

When you make an NFC payment, Microsoft Wallet will provide the merchant with an encrypted version of your payment card (a "token"). The merchant will present this token, along with transaction details, to your bank to complete the transaction and request payment for your transaction.

Windows Hello

Windows Hello provides instant access to your devices through biometric authentication. If you turn it on, Windows Hello uses your face, fingerprint, or iris to identify you based on a

set of unique points or features that are extracted from the image and stored on your device as a template - but it does not store the actual picture or image of your face or iris. Biometric verification data that's used when you sign in doesn't leave your device. You can delete your biometric verification data from within Settings.

Windows Media Player

Windows Media Player allows you to play CDs, DVDs and other digital content (such as WMA and MP3 files), rip CDs, and manage your media library. To enrich your experience when you play content in your library, Windows Media player displays related media information, such as album title, song titles, album art, artist and composer. To augment your media information, Windows Media player will send a request to Microsoft which contains standard computer information, an identifier for the media content, and the media information already contained in your Windows Media Player library (including information you may have edited or entered yourself) so that Microsoft can recognize the track and then return additional information that is available.

Windows Media Player also allows you to play back content that is streamed to you over a network. To provide this service, it is necessary for Windows Media Player to communicate with a streaming media server. These servers are typically operated by non-Microsoft content providers. During playback of streaming media, Windows Media Player will send a log to the streaming media server or other web server(s) if the streaming media server requests it. The log includes such details as: connection time, IP address, operating system version, Windows Media Player version, Player identification number (Player ID), date, and protocol. To protect your privacy, Windows Media Player defaults to sending a Player ID that is different for each session.

Windows Search

Windows Search lets you search your stuff and the web from one place. If you choose to use Windows Search to search "your stuff", it will provide results for items on your personal OneDrive, your OneDrive for Business if so enabled, other cloud storage providers to the extent supported by those third-party providers, and on your device. If you choose to use Windows Search to search the web, or get search suggestions with Windows Search or Cortana, your search results will be powered by Bing and we will use your search query as described in the [Bing](#) section of this privacy statement.

Xbox

Xbox consoles are hardware devices that you can use to access and play games, movies, music, and other forms of digital entertainment. Xbox Live (including Games for Windows Live) is Microsoft's online gaming and entertainment service and social network. It provides ways for you to connect with your friends on Xbox Live and other gaming and social networks. Xbox services can be accessed from a variety of devices, including Xbox consoles, PCs (including via xbox.com and the Xbox app), and mobile devices.

We collect data about your use of Xbox services, such as:

- When you sign in and sign out, the games you play, your game and score statistics, and the purchases you make and content you obtain.
- Performance data about the Xbox services, your device and your network connection, including any hardware or software errors that occur.
- If you use the Xbox console with Kinect, data about how you use Kinect. See below for more information about Kinect data collection.

All such data is stored with the Xbox console's unique identifier and associated with your personal data. When your Xbox is connected to the Internet, we identify which console and which version of the Xbox operating system you are currently using.

With your consent, we will collect information about videos you purchase or view through third-party apps on your Xbox console. If you use the Xbox TV app, we collect TV viewing history from your console in a way that doesn't identify you or others.

If you use an Xbox console that includes a storage device (hard drive or memory unit), and if you play offline or have never signed into the services on the console, usage data will be stored on the storage device and sent to Microsoft the next time you sign into the services.

Xbox Live data viewable by other users. Your gamertag (Xbox live nickname), game and score statistics, achievements, presence (whether you're signed into Xbox Live), and other data about your activity on Xbox Live can be seen by other users on Xbox Live or other properties associated with Xbox Live (including those of partner companies). For example, your gamertag and scores that show on game leaderboards are considered public and can't be hidden. For other types of data, you can adjust your privacy settings on the console or at xbox.com to limit or block the sharing with other users.

Xbox Live data shared with game or app publishers. When you use an Xbox Live-enabled game or app, the publisher or service provider for that game or app has access to data about your usage of Xbox Live and that game or app, and may disclose or display (such as on leaderboards) such data. This data includes, for example, your game scores, data about your game play sessions (for example, types of vehicles used in the game), your presence on Xbox Live, the time you spend playing the game or app, rankings, statistics, gamer profiles, avatars, and other content that you may create or submit within the game or app.

Linking your Xbox Live account to non-Microsoft accounts. Some of the games or apps found on Xbox Live are delivered by partner companies, which may require that you create a non-Microsoft account and sign-in credentials to use that game or app. If you choose to link your Microsoft account with your account with a partner company, Microsoft will share limited account information with that company. Such account information can include name, address, email and date of birth but will not include any credit card or other payment information. For games that enable in-game communications, the game publisher will also have access to the content of in-game communications when you are signed into your account with the publisher.

Kinect. The Kinect sensor is a combination of camera, microphone, and infrared sensor that can enable motions and voice to be used to control gameplay and to navigate through the service. For example:

- If you choose, the camera can be used to sign you into the service automatically using facial recognition. To do this it takes an image of your face and measures distances between key

points to create and store a numeric value that represents only you. This data stays on the console and is not shared with anyone, and you can choose to delete this data from your console at any time.

- For gameplay, Kinect will map distances between your body's joints to create a stick figure representation of you that helps Kinect enable gameplay. If you are playing online, we collect those numeric values to enable and improve gameplay and the gaming experience. Kinect also detects specific hand gestures intended to do simple system interactions (such as menu navigation, pan/zoom and scroll).
- For some fitness games, Xbox can use the Kinect sensor to estimate your exercise data, including estimates such as your heart rate during a certain activity or the number of calories burned during a workout.
- Kinect's microphones enable voice chat between players during gameplay. They also enable voice commands for control of the console, game or app, or to enter search terms. See below for additional details on voice data collection.
- The Kinect sensor can also be used for audio and video communications through services such as [Skype](#).

To learn more about Kinect, for Xbox 360, see [Kinect and Xbox 360 privacy](#). For Xbox One, see [Kinect and Xbox One Privacy](#).

Captioning. During Xbox real-time chat, players may activate a voice-to-text feature, which allows the user to view the audio in-game chat as text. If a user activates this feature, the other players will have no additional notice. Microsoft uses this data to provide captioning of chat for users who need it. We also use this data to improve our ability to provide the service and other, similar voice-based services.

Communications monitoring. Xbox Live includes communications features such as text-based messaging and online voice chat between players during gameplay. In order to help provide a safe gaming environment and enforce the [Microsoft Code of Conduct](#), we will collect, review, and monitor a sample of these communications, including Xbox Live game chats and party chat communications in live-hosted multiplayer gameplay sessions offered through the services.

Voice data for service improvement. We collect, and use for service improvement, voice search requests or samples of voice commands occurring while using Kinect. These data are stored separately from your Xbox profile.

GameDVR. Any player in a multiplayer game session can use GameDVR to record their view of the gameplay taking place in that session. The recording can capture your in-game character and gamertag in the game clips created by other players in the gameplay session. Note that if a player uses GameDVR on a PC, audio chat may also be captured in a game clip. Microsoft can review game clips for violations of the [Microsoft Code of Conduct](#), even if your game clip sharing setting is set to Block.

Xbox Live Rewards. Xbox Live Rewards, available at [rewards.xbox.com](#), is a program you can join to receive Xbox credits for being active on the services. You must agree to receive promotional communications from the Rewards program as a condition of joining. You sign into Rewards using your Microsoft account, and the program collects personal data including first name, last name, gamertag, and demographic information. The program is hosted and operated by HelloWorld, a Microsoft vendor. The data collected is stored by the vendor on behalf of Microsoft. You can review and edit the personal data you provided to the Rewards program by contacting [privacy@helloworld.com](#).

Children and online safety. If you have children who use Xbox services, you can set up child accounts for them. Children 17 and younger cannot create an account on Xbox Live without parental consent. Adults in the family can change consent choices and online safety settings for child accounts on xbox.com.

Enterprise Products

Enterprise Products are those Microsoft products and related offerings that are offered or designed primarily for use by organizations and developers. They include subscription cloud services, such as Office 365, Microsoft Azure, Microsoft Dynamics CRM Online, Microsoft Intune, and Yammer, for which an organization (our "customer") contracts with Microsoft for the services ("Online Services"). They also include server and developer products customers run on their own premises, such as Windows Server, SQL Server, Visual Studio, and System Center ("On-Prem Products"). Microsoft Cognitive Services are not Enterprise Products under this privacy statement.

Some Enterprise Products have their own, separate privacy statements. The following notices explain specific privacy practices with respect to certain Microsoft products you may use:

- [Enterprise and developer](#)
- [Online services](#)

In the event of a conflict between a Microsoft privacy statement and the terms of any agreement(s) between a customer and Microsoft, the terms of those agreement(s) will control.

When a customer purchases or subscribes to Enterprise Products, or obtains support for such products, Microsoft collects data to provide the best experiences with our products, operate our business, and communicate with the customer. For example:

- When a customer engages with a Microsoft sales representative, we collect the customer's name and contact data, along with information about the organization, to support that engagement.
- When a customer interacts with a Microsoft support professional, we collect support data or error reports to diagnose and resolve problems.
- When a customer pays for products, we collect contact and payment data to process the payment.
- When a customer receives communications for Microsoft, we use data to personalize the content of the communication.

Our customers, in turn, may administer the Enterprise Products to end users. If you use a work or school account (i.e. an email address provided by your organization, such as your employer or school) to sign into Enterprise Products, the owner of the domain associated with your email address may: (i) control and administer your account and (ii) access and process your data, including the contents of your communications and files. Microsoft is not responsible for the privacy or security policies or practices of our customers, which may differ from those of Microsoft. If your organization is administering your use of the Enterprise Products, please direct your privacy inquiries to your administrator.

Online Services. The Online Services collect Customer Data and Administrator Data. "Customer Data" means all data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, you or your end users through use of the Online Service. Customer

Data is used only to provide the customer the Online Services including purposes compatible with providing those services. For example, we may use Customer Data to provide a personalized experience, improve service reliability, combat spam or other malware, or improve features and functionality of the Online Services. Microsoft will not use Customer Data or derive information from it for any advertising or similar commercial purposes. For more information about the features and functionality that enable you to control Customer Data, please review documentation specific to the Online Service. To learn more about Microsoft's handling of Customer Data, including information about how we handle data access requests and security, please see [Microsoft Online Services Terms](#).

“Administrator Data” is data provided to Microsoft during sign-up, purchase, or administration of the Online Services. Administrator Data includes the name, address, phone number, and email address you provide, as well as aggregated usage data related to your account, such as the controls you select. We use Administrator Data to provide the Online Services, complete transactions, service the account, and detect and prevent fraud. Administrator Data may also include contact information of your colleagues and friends if you agree to provide it to Microsoft for the limited purpose of sending them an invitation to use the Online Services; we may contact those individuals with communications that may include information about you, such as your name and profile photo.

As needed, we use Administrator Data to contact you to provide information about your account, subscriptions, billing, and updates to the Online Services, including information about new features, security or other technical issues. We may also contact you regarding third-party inquiries we receive regarding use of the Online Services, as described in your agreement. You will not be able to unsubscribe from these non-promotional communications. Subject to your contact preferences, we may also contact you regarding information and offers about other products and services, or share your contact information with Microsoft's partners. You may manage your contact preferences or update your information in your account profile.

When you use social features of the Online Services, other users in your network may see some of your activity. To learn more about the social features and other functionality, please review documentation specific to the Online Service.

The Online Services enable you to purchase, subscribe to or use other Microsoft products. Please be sure to read the product-specific details for each product you use to understand how each products' privacy practices may differ.

On-Prem Products. On-Prem Products collect data to operate effectively and provide you the best experiences. The data we collect depends on the features you use, but it is generally limited to usage data. Customers have choices about the data they provide. For example:

- During installation or when you upgrade an On-Prem Product, we may collect use and performance data to learn whether you experience any difficulties.
- When you use On-Prem Products, we may collect device data to learn about your operating environment to improve security features.
- When you experience a crash, you may choose to send Microsoft an error report to help us diagnose the problem and deliver customer support.

Microsoft uses the data we collect from On-Prem Products to provide and improve our products, to deliver customer support, to activate the product, to communicate with you, and to operate our business.

- [Contact us](#)
- [Privacy and cookies](#)
- [Terms of use](#)
- [Trademarks](#)
- [About our ads](#)
- © Microsoft 2017



Change History for Microsoft Privacy Statement

[Back to the privacy statement](#)

June 2017

- We made a small update to the language in **Privacy Shield** to highlight that Microsoft participates in both the EU-U.S. and the Swiss-EU Privacy Shield frameworks.

March 2017

- We updated **Personal Data We Collect** to provide customers with more transparency about the types of third parties that provide us with personal data. Additionally, we made edits to better describe the types of data we collect.
- Under **How We Use Personal Data**, we clarified to customers how we use information about their activities, interests, and location to deliver personalized experiences.
- In **How to Access & Control Your Personal Data**, we added information about the new Microsoft privacy dashboard, where customers can access and manage personal data collected from various Microsoft services. We added details about where users can delete their personal data on other Microsoft properties.
- We added AppsFlyer to the list of analytics providers in **Cookies & Similar Technologies**.
- We updated **Microsoft Account** to provide customers with information about how our new payment features work.
- We added a new section called **European Privacy Rights** to inform customers in the European Economic Area of their data protection rights.
- In **Where We Store and Process Personal Data** we provided customers with more information about where Microsoft processes data. We specified where Microsoft operates major data centers and explained how we determine where we process data. Additionally, we provided more transparency about transfers of personal data from the European Economic Area, including the legal basis for such transfers and how we protect customers' rights when the data travels. We set forth our commitment to the EU-U.S. and the Swiss-U.S. Privacy Shield frameworks and direct customers on how they can exercise their Privacy Shield rights.
- As we seek to be more transparent about how long we keep personal data, we set forth criteria we use to determine retention periods in **Our Retention of Personal Data**.
- Under **Bing**, we provided more clarity to customers about how to turn off Search Suggestions, pointed customers to new capabilities to manage their data, and added details about how search query data is used for research and development purposes.

- In **Cortana**, we added information to describe how new features work. We explained variations of Cortana on different operating systems and how Cortana interacts with other services. Additionally, we provided more information about how we use location information and moved information about Cortana's use of information from Microsoft Edge up from the **Windows** section.
- In **Health Services**, we made edits for clarity and to account for new applications in this product area.
- We updated **MSN** to better clarify the type of data collected to provide customers with relevant content.
- In **Office** we edited the structure of one sentence to make it more clear.
- Under **Windows** we made a number of changes to improve transparency, to describe changes to certain functionality or new capabilities, and to account for new privacy measures we implemented, including:
 - Under **Advertising ID**, we explained how customers can control the use of this identifier and provided more clarity on how app developers and advertising networks use it.
 - We renamed *Telemetry and Error Reporting* to **Diagnostics**. In this section, we explained the two levels of diagnostic data, including the type of data collected for each level, depending on the customer's setting. Additionally, we explained the new **Tailored Experiences** setting, which enables users to choose whether diagnostic data is used to personalize their experience.
 - We provided more clarity on the collection of location data in **Windows location service**.
 - In **Recording**, we described new capabilities and informed users of their potential legal responsibility related to the use of this feature.
 - In **SmartScreen**, we provided additional details about the data transmitted to Microsoft to help SmartScreen protect customers.
 - In **Speech, Inking and Typing**, we better described our speech recognition capabilities and provided more transparency about the data Microsoft collects to provide these and related services. Additionally, we explained to customers the controls available to manage this data.
 - Under **Web Browsers** we removed references to **Page Prediction**. The Page Prediction feature still exists in Microsoft browsers. However, browsing history to power the feature is now collected as part of Windows Diagnostics only from devices configured to return data at the Full level. We also moved disclosures about Cortana's use of data from this section to the **Cortana** section.
 - We renamed **Windows Wi-Fi Sense** section to **Wi-Fi Connecting to suggested open hotspots** and edited this section to reflect changed branding and features.
 - We clarified **Microsoft Wallet** is an application only available for Windows Phone by renaming this section.
 - We added a section for **Windows Media Player** to describe how this feature works for versions of Windows where this application is available.
 - We edited **Windows Search** to describe how the feature can be used to search for items stored in other services.
- In some language versions, we made edits for grammar.

February 2017

- In **Personal Data We Collect**, we clarified additional details about the usage data we consider “Product use data.”
-

November 2016

- In **How We Use Personal Data**, we updated **Advertising** to better clarify the use of your data by third parties to customize the ads you see.
 - In **How to Access & Control Your Personal Data**, we updated **Your Communications Preferences**, clarifying how to modify your preferences.
 - In **Other Important Information**, we updated the **Where We Store and Process Personal Data** section to reflect Microsoft’s participation in the EU-U.S. Privacy Shield program.
 - In **Bing**, we removed the Bing Rewards Program section, as Bing Rewards has been replaced by Microsoft Rewards.
 - We added a new **Microsoft Cognitive Services** section to explain how we collect and use data when developers use the services. We also clarified that Microsoft Cognitive Services are not Enterprise Products under this privacy statement.
 - We added a new **Microsoft Translator** section, to explain how Microsoft Translator, Collaborative Translations Framework, and Microsoft Translator Hub collect and use data.
 - In **Windows**, we revised the **Telemetry & Error Reporting** section to reflect that wireless network identifiers are collected at the optional “Enhanced” level of telemetry rather than at the “Basic” level.
 - We added a new **captioning** section in **Xbox** to explain how Microsoft incorporates a voice-to-text feature to provide captioning of in-game chat for users who need it.
-

September 2016

In **Enterprise Products**, we added links to privacy notices that still apply to certain enterprise offerings.

August 2016

- In **Personal Data We Collect**, we added additional examples of when we collect data and the types of usage data we collect.
- In **How We Use Personal Data**:
 - We clarified that we show ads in only some of our products, that we also deliver ads in third-party products, and that we partner with third-parties such as AOL and AppNexus to deliver ads. And we removed an outdated example of sharing data with a service provider to help with the delivery of ads.
 - We added additional examples of using data for product improvement purposes.
- In **Microsoft account**:
 - We added text explaining the distinctions between a personal Microsoft account and a work or school account provided by your school or employer using Azure Active Directory.

- We added an explanation that when you sign into a third-party product with your Microsoft account, and consent to share profile data, the third-party product can display your name or username and profile photo.
- In **Other Important Information**, we updated the discussion of transferring data from the European Economic Area to specify our intent to adopt the forthcoming EU-U.S. Privacy Shield Principles.
- In **Cortana**, we provided more examples of the types of data Cortana can access and use, described a new feature that allows for some functionality without being signed in, described new and enhanced user controls, and added descriptions (already provided to users in the product itself) of data sharing with third-party services that users can choose to connect with Cortana.
- In **Microsoft Health and Microsoft Band**, we added more detail about the types of data these offerings collect and use, and removed some redundant text to simplify the section.
- We added a new **Outlook** section (incorporating content previously in an Outlook.com section and an Outlook subsection of Office) to explain the distinctions between Outlook.com, Outlook applications, and related services, describe new cloud-based features, and describe how Outlook applications can be integrated with multiple accounts from third-party service providers.
- In **Skype**, we added text explaining that this section applies only to the consumer version of Skype and not Skype for Business, describing how contacts are added to Skype from other Microsoft consumer services, and describing a new recording feature in some versions of Skype.
- We added a new **Store** section, incorporating the content previously in a Windows Store subsection of Windows, and adding references to the Xbox Store and Office Store.
- We added a new **SwiftKey** section to describe our recently acquired SwiftKey apps, incorporating the content from the previous SwiftKey privacy statement.
- In **Windows**:
 - We expanded the description of **Advertising ID** to provide more details on its purpose and uses.
 - We renamed the "Input Personalization" section to **Speech, Inking, and Typing** and added additional examples of the data collected.
 - In **Location Services, Motion Sensing, and Recording**, we added descriptions of the new **General location** and **Default location** settings, and provided additional details of when location data is collected and retained by Microsoft.
 - We updated the **Windows Defender** section to explain new functionality that allows the use of Windows Defender to do periodic scanning even when there is another anti-malware service running.
 - We've revised the **Telemetry & Error Reporting** section to further clarify differences between **Basic** data, **Enhanced** data, and **Full** data.
 - We updated the **Web Browsers: Microsoft Edge and Internet Explorer** section to explain how to control Cortana's access to your browsing history, and that enabling that feature will allow us to collect your Microsoft Edge search queries and full browsing history associated with your user ID to personalize your experience.
 - We revised the **Wi-Fi Sense** section to clarify that we are no longer offering functionality that will automatically connect to open Wi-Fi networks.
 - We added a section to **Windows Apps** describing the Mail and Calendar app, and updated the description of the Microsoft Wallet app to reflect to NFC functionality.
- We added a new **Enterprise Products** section (replacing an Enterprise Services subsection of **Other Important Information**) to account for Microsoft products and related offerings offered or designed primarily for use by organizations and developers.

- Throughout, we replaced the general term "services" with "products" to better reflect the full range of software, services, and devices Microsoft offers.
 - Throughout, we made several minor wording changes to improve clarity, or to address typos, grammar, or other similar issues.
-

January 2016

- We simplified the introductory paragraph by removing a list of specific Microsoft services, referring instead to the list of services that appears later in the statement.
 - In **Microsoft account**, we added “display name” to the ways others can find and connect with you within Microsoft services.
 - In **Other Important Privacy Information**:
 - In **Where We Store and Process Personal Data**, we clarified that data may be stored in your region, and explained the ways data can be transferred from the European Economic Area to other countries.
 - We simplified **How to Contact Us** by removing the reference to Skype Software S.à.r.l.
 - In **Skype**, we made several edits to simplify and clarify language, remove redundancies, and explain that both Microsoft Corporation and Skype Communications S.à.r.l. are data controllers for Skype.
 - In **Windows**:
 - We added to **Sync Settings**, to clarify that the Windows sync settings apply to Internet Explorer browser history, and that some apps have their own separate sync controls.
 - We rewrote much of **Telemetry & Error Reporting** to clarify the different levels of telemetry, what types of data are included in each, the effect of the available user controls, and the limited sharing of error report information to partners (such as OEMs) to help them troubleshoot products and services which work with Windows and other Microsoft product and services.
 - We clarified **Web Browsers** to show the differences between sync functions and controls on Internet Explorer and Microsoft Edge.
 - Throughout, we made several minor wording changes to improve clarity, or to address typos, grammar, or other similar issues.
-

October 2015

- We added examples to **Personal Data We Collect** to clarify when we need to collect content of files and communications so that we can provide our services to you.
- We added examples to **How We Use Personal Data** about customer support and product activation, to further explain how we use your data to provide and improve our services.
- In **Reasons We Share Personal Data**, we clarified that “private communications and documents in private folders” refers to content in cloud services, like Outlook.com and OneDrive, and not content stored on a person’s local device. We also added a link to our Law Enforcement Transparency Report.
- In **Cookies and Other Technologies**, we added Kissmetrics and Webtrends to the list of data analytics service providers we use.
- We clarified the difference between a personal **Microsoft account** and a work or school account provided to you by your organization.

- In **Other Important Privacy Information**, we added **Enterprise Services** to clarify that if you have a work or school account, the owner of the domain associated with your email address may control and administer your account under its own policies, which may differ from ours.
 - In **Bing**, we updated “Autosuggest” to “Search Suggestions” and added information about how to opt out of Bing Rewards.
 - In **Cortana**, we added “Communications History” to the list of features.
 - We added **Groove Music/Movies & TV**, which replaces **Xbox Music and Video** to reflect the new branding of those services.
 - We added **Microsoft Health Services**, to incorporate information previously provided in separate privacy statements about Microsoft Band devices, Microsoft Health apps, HealthVault, and other related services.
 - We simplified Office, by moving the pertinent information from the old **Excel** subsection into **Search services**.
 - In **Outlook**, we deleted **Social inbox**.
 - In Skype, we added information about **Translation feature**.
 - In Windows, we added information about **Recording**.
 - In **Xbox**, we changed **Voice chat** to **Communications monitoring**. We also clarified that the Xbox Code of Conduct has been replaced with the Microsoft Code of Conduct.
 - Throughout, we made several minor wording changes to improve clarity, or to address typos, grammar, or other similar issues.
-

July 2015

We published a new Microsoft Privacy Statement that brought together many separate privacy statements into a single statement covering most of Microsoft’s consumer services. This restructuring of Microsoft’s privacy disclosures was designed to eliminate redundancies, improve usability, and increase clarity and transparency. We added some new elements, for example, to reflect new features of Windows 10, but the new statement did not represent a change in policy or practice for Microsoft.

- [Contact us](#)
- [Privacy and cookies](#)
- [Terms of use](#)
- [Trademarks](#)
- [About our ads](#)
- © Microsoft 2017